ID: 652395
Sample Name: yIF7nMz573.exe
Cookbook: default.jbs
Time: 09:45:34
Date: 26/06/2022
Version: 35.0.0 Citrine

Table of Contents

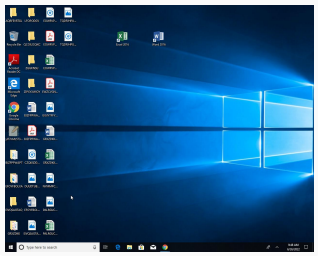
Windows Analysis Report

yIF7nMz573.exe

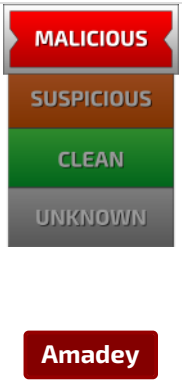
Overview

General Information

Sample Name:	yIF7nMz573.exe
Analysis ID:	652395
MD5:	dce2a8f4ab6087..
SHA1:	c889640843424e..
SHA256:	2be50564951116.
Tags:	Amadey exe
Infos:	



Detection



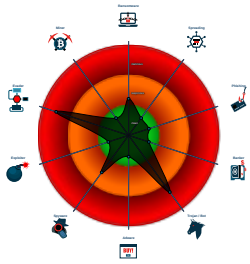
Amadey

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

Signatures

- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected Amadey bot
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Machine Learning detection for sam…
- Contains functionality to inject code…
- Creates an undocumented autostart…
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- yIF7nMz573.exe (PID: 6472 cmdline: "C:\Users\user\Desktop\yIF7nMz573.exe" MD5: DCE2A8F4AB60879898A21AB451CAD63F)
  - bguuwe.exe (PID: 6608 cmdline: "C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe" MD5: DCE2A8F4AB60879898A21AB451CAD63F)
    - cmd.exe (PID: 6764 cmdline: "C:\Windows\System32\cmd.exe" /C REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\Users\user\AppData\Local\Temp\62eca45584\ MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6776 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - reg.exe (PID: 6816 cmdline: REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\Users\user\AppData\Local\Temp\62eca45584\ MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - schtasks.exe (PID: 6784 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN bguuwe.exe /TR "C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- bguuwe.exe (PID: 6960 cmdline: C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe MD5: DCE2A8F4AB60879898A21AB451CAD63F)
- bguuwe.exe (PID: 6504 cmdline: C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe MD5: DCE2A8F4AB60879898A21AB451CAD63F)
- **cleanup**

Malware Configuration

Threatname: Amadey


```
{
  "C2 url": "185.215.113.15/Lkb2dxj3/index.php",
  "Version": "3.21"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15

Timestamp:	192.168.2.3185.215.113.1549746802027700 06/26/22-09:46:57.610393
SID:	2027700
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15

Timestamp:	192.168.2.3185.215.113.1549749802027700 06/26/22-09:47:01.350218
SID:	2027700
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15

Timestamp:	192.168.2.3185.215.113.1549798802027700 06/26/22-09:47:41.864054
SID:	2027700
Source Port:	49798
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15

Timestamp:	192.168.2.3185.215.113.1549832802027700 06/26/22-09:48:33.213243
SID:	2027700
Source Port:	49832
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15

Timestamp:	192.168.2.3185.215.113.1549755802027700 06/26/22-09:47:21.773924
SID:	2027700
Source Port:	49755
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15

Timestamp:	192.168.2.3185.215.113.1549826802027700 06/26/22-09:48:24.530301
SID:	2027700
Source Port:	49826
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549829802027700 06/26/22-09:48:27.114493
SID:	2027700
Source Port:	49829
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549841802027700 06/26/22-09:48:43.294919
SID:	2027700
Source Port:	49841
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549780802027700 06/26/22-09:47:27.628822
SID:	2027700
Source Port:	49780
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549767802027700 06/26/22-09:47:22.040844
SID:	2027700
Source Port:	49767
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549761802027700 06/26/22-09:47:20.297421
SID:	2027700
Source Port:	49761
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549801802027700 06/26/22-09:47:44.118576
SID:	2027700
Source Port:	49801
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549776802027700 06/26/22-09:47:25.997227
SID:	2027700
Source Port:	49776
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549810802027700 06/26/22-09:47:57.512185

SID:	2027700
Source Port:	49810
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549773802027700 06/26/22-09:47:23.164370
SID:	2027700
Source Port:	49773
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549758802027700 06/26/22-09:47:18.795200
SID:	2027700
Source Port:	49758
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549782802027700 06/26/22-09:47:29.252532
SID:	2027700
Source Port:	49782
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549756802027700 06/26/22-09:47:13.646635
SID:	2027700
Source Port:	49756
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549785802027700 06/26/22-09:47:30.265752
SID:	2027700
Source Port:	49785
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549828802027700 06/26/22-09:48:25.611929
SID:	2027700
Source Port:	49828
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549816802027700 06/26/22-09:48:09.646530
SID:	2027700
Source Port:	49816
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549845802027700 06/26/22-09:48:46.784890
SID:	2027700
Source Port:	49845
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549774802027700 06/26/22-09:47:24.256337
SID:	2027700
Source Port:	49774
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549839802027700 06/26/22-09:48:37.748469
SID:	2027700
Source Port:	49839
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549797802027700 06/26/22-09:47:41.469763
SID:	2027700
Source Port:	49797
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549817802027700 06/26/22-09:48:11.724189
SID:	2027700
Source Port:	49817
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549786802027700 06/26/22-09:47:30.623905
SID:	2027700
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549745802027700 06/26/22-09:46:54.779771
SID:	2027700
Source Port:	49745
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549757802027700 06/26/22-09:47:16.401762

SID:	2027700
Source Port:	49757
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549823802027700 06/26/22-09:48:17.269325
SID:	2027700
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549751802027700 06/26/22-09:47:05.409898
SID:	2027700
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549781802027700 06/26/22-09:47:28.674122
SID:	2027700
Source Port:	49781
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549805802027700 06/26/22-09:47:48.812945
SID:	2027700
Source Port:	49805
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549775802027700 06/26/22-09:47:25.180668
SID:	2027700
Source Port:	49775
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549803802027700 06/26/22-09:47:47.323846
SID:	2027700
Source Port:	49803
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549812802027700 06/26/22-09:47:59.897990
SID:	2027700
Source Port:	49812
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549806802027700 06/26/22-09:47:54.097536
SID:	2027700
Source Port:	49806
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549784802027700 06/26/22-09:47:30.001407
SID:	2027700
Source Port:	49784
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549787802027700 06/26/22-09:47:30.877538
SID:	2027700
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549793802027700 06/26/22-09:47:39.471421
SID:	2027700
Source Port:	49793
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549796802027700 06/26/22-09:47:40.783332
SID:	2027700
Source Port:	49796
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549799802027700 06/26/22-09:47:42.867694
SID:	2027700
Source Port:	49799
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549830802027700 06/26/22-09:48:30.483127
SID:	2027700
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549818802027700 06/26/22-09:48:13.810900

SID:	2027700
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549744802027700 06/26/22-09:46:53.237130
SID:	2027700
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549815802027700 06/26/22-09:48:05.618223
SID:	2027700
Source Port:	49815
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549842802027700 06/26/22-09:48:44.262889
SID:	2027700
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549791802027700 06/26/22-09:47:37.619364
SID:	2027700
Source Port:	49791
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549824802027700 06/26/22-09:48:18.293793
SID:	2027700
Source Port:	49824
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549833802027700 06/26/22-09:48:36.596810
SID:	2027700
Source Port:	49833
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	−
Timestamp:	192.168.2.3185.215.113.1549750802027700 06/26/22-09:47:03.761613
SID:	2027700
Source Port:	49750
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549809802027700 06/26/22-09:47:55.667044
SID:	2027700
Source Port:	49809
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549825802027700 06/26/22-09:48:19.702891
SID:	2027700
Source Port:	49825
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549788802027700 06/26/22-09:47:31.215612
SID:	2027700
Source Port:	49788
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549794802027700 06/26/22-09:47:42.618057
SID:	2027700
Source Port:	49794
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549753802027700 06/26/22-09:47:07.860735
SID:	2027700
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549747802027700 06/26/22-09:46:59.493020
SID:	2027700
Source Port:	49747
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549813802027700 06/26/22-09:48:02.729973
SID:	2027700
Source Port:	49813
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549765802027700 06/26/22-09:47:21.494001

SID:	2027700
Source Port:	49765
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549742802027700 06/26/22-09:46:52.260106
SID:	2027700
Source Port:	49742
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549777802027700 06/26/22-09:47:26.632947
SID:	2027700
Source Port:	49777
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549783802027700 06/26/22-09:47:29.721183
SID:	2027700
Source Port:	49783
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549790802027700 06/26/22-09:47:31.866868
SID:	2027700
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549802802027700 06/26/22-09:47:45.689140
SID:	2027700
Source Port:	49802
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549789802027700 06/26/22-09:47:31.596641
SID:	2027700
Source Port:	49789
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549754802027700 06/26/22-09:47:11.567118
SID:	2027700
Source Port:	49754
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549795802027700 06/26/22-09:47:39.970739
SID:	2027700
Source Port:	49795
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 185.215.113.15	
Timestamp:	192.168.2.3185.215.113.1549820802027700 06/26/22-09:48:15.889921
SID:	2027700
Source Port:	49820
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Compliance

- Detected unpacking (overwrites its own PE header)

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

Data Obfuscation

- Detected unpacking (overwrites its own PE header)
- Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

- Yara detected Amadey bot

Boot Survival

- Creates an undocumented autostart registry key
- Uses schtasks.exe or at.exe to add and modify task schedules

HIPS / PFW / Operating System Protection Evasion

Contains functionality to inject code into remote processes

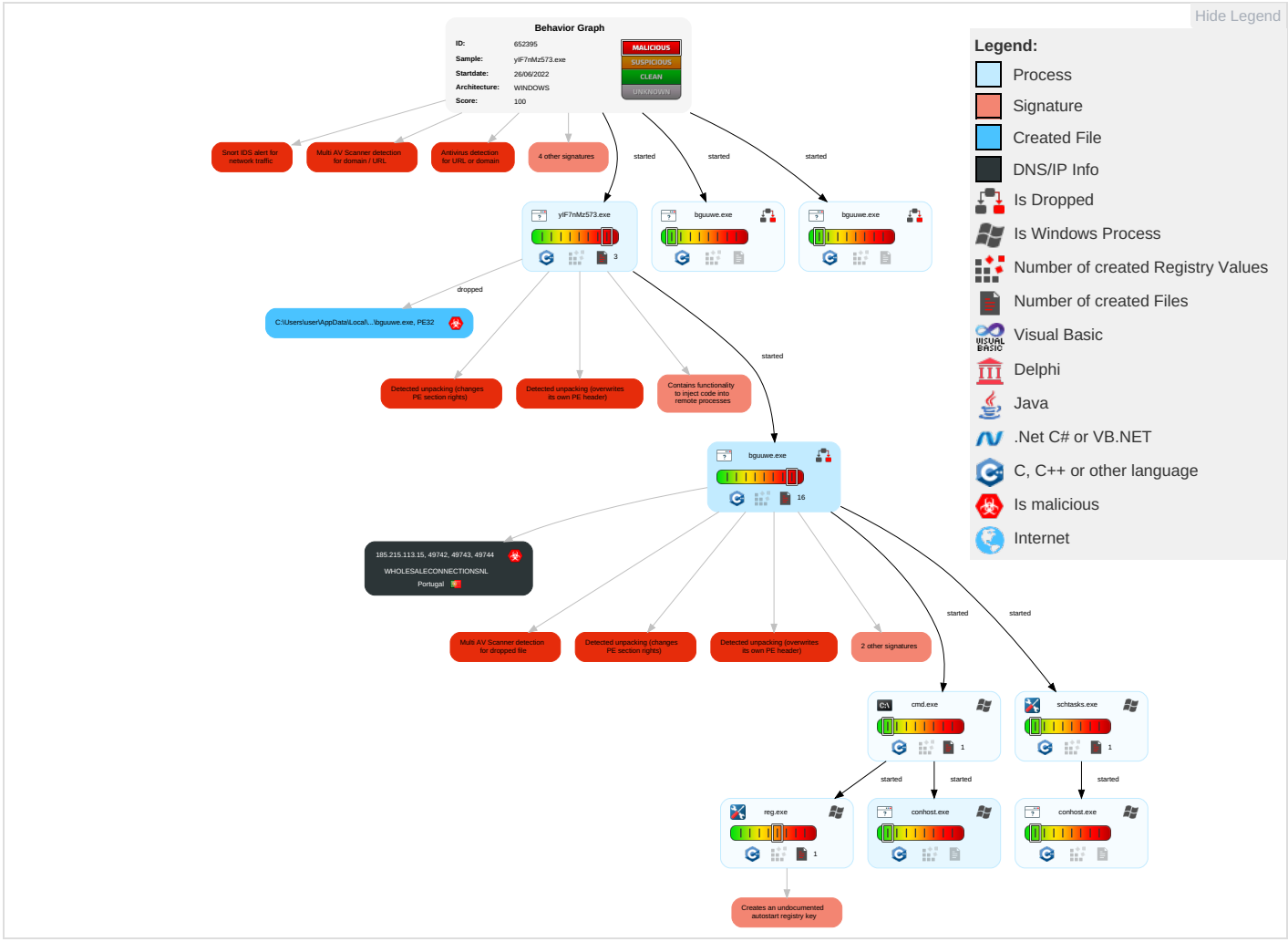
Stealing of Sensitive Information

Yara detected Amadey bot

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	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 1 Process Injection	1 Masquerading	1 Input Capture	2 System Time Discovery	Remote Services	1 Screen Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Modify Registry	LSASS Memory	1 2 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	4 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 1 Virtualization/Sandbox Evasion	Security Account Manager	1 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 System Owner/User Discovery	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	2 Software Packing	DCSync	2 File and Directory 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	Indicator Removal from Tools	Proc Filesystem	2 4 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

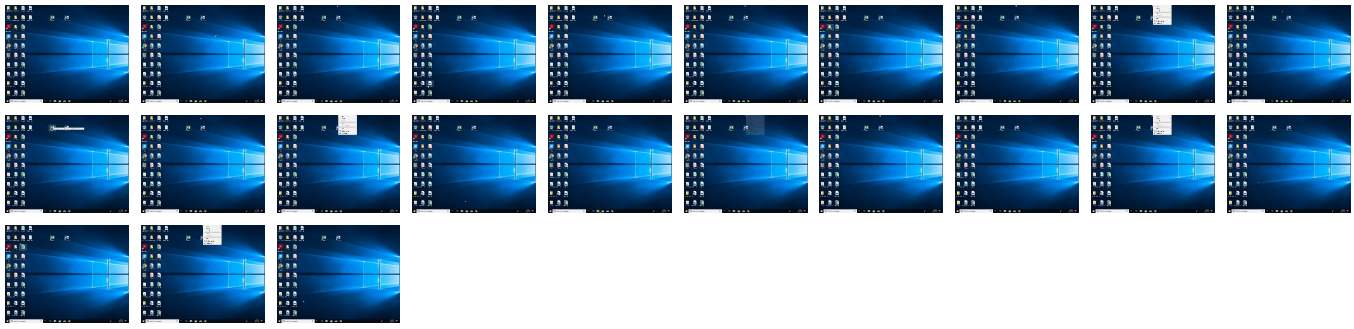
Behavior Graph



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
yIF7nMz573.exe	37%	Virustotal		Browse
yIF7nMz573.exe	46%	ReversingLabs	Win32.Trojan.DllCheck	
yIF7nMz573.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe	46%	ReversingLabs	Win32.Trojan.DllCheck	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.yIF7nMz573.exe.e40000.0.unpack	100%	Avira	HEUR/AGEN.1215503		Download File
10.3.bguuwe.exe.2680000.0.unpack	100%	Avira	HEUR/AGEN.1215503		Download File
1.3.bguuwe.exe.f10000.0.unpack	100%	Avira	HEUR/AGEN.1215503		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.yIF7nMz573.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1237910		Download File
19.2.bguuwe.exe.dc0e67.1.unpack	100%	Avira	HEUR/AGEN.1215503		Download File
0.2.yIF7nMz573.exe.cb0e67.1.unpack	100%	Avira	HEUR/AGEN.1215503		Download File
19.3.bguuwe.exe.1010000.0.unpack	100%	Avira	HEUR/AGEN.1215503		Download File
10.2.bguuwe.exe.ca0e67.1.unpack	100%	Avira	HEUR/AGEN.1215503		Download File
19.2.bguuwe.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1237910		Download File
10.2.bguuwe.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1237910		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.215.113.15/Lkb2dxj3/cred.dll	11%	Virustotal		Browse
http://185.215.113.15/Lkb2dxj3/cred.dll	100%	Avira URL Cloud	malware	
http://185.215.113.15/Lkb2dxj3/index.php?scr=1	17%	Virustotal		Browse
http://185.215.113.15/Lkb2dxj3/index.php?scr=1	100%	Avira URL Cloud	malware	
http://185.215.113.15/Lkb2dxj3/index.php	8%	Virustotal		Browse
http://185.215.113.15/Lkb2dxj3/index.php	100%	Avira URL Cloud	malware	
185.215.113.15/Lkb2dxj3/index.php	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.215.113.15/Lkb2dxj3/cred.dll	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://185.215.113.15/Lkb2dxj3/index.php?scr=1	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://185.215.113.15/Lkb2dxj3/index.php	true	• 8%, Virustotal, Browse • Avira URL Cloud: malware	unknown
185.215.113.15/Lkb2dxj3/index.php	true	• Avira URL Cloud: malware	low

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.215.113.15	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	652395
Start date and time: 26/06/202209:45:34	2022-06-26 09:45:34 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yIF7nMz573.exe
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:	26
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.evad.winEXE@13/3@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:46:51	API Interceptor	2360x Sleep call for process: bguuwe.exe modified
09:46:53	Task Scheduler	Run new task: bguuwe.exe path: C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe

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\Temp\425620883392

Process:	C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	95220
Entropy (8bit):	7.918649658368608

Encrypted:	false
SSDEEP:	1536:CMhgLEkW/50z3KBo0OWKPkuzQugrNyCdsRwzUQ8+HUQhjWRZ95/fVMzW3rs4V/oV:lhHkWx0zyjKTzQDdsvQQfVMzmr1/E
MD5:	3A84660401E612C2322E89C892946CA5
SHA1:	7ED38353BE6606E17997B21E9CBEDFFACD38385A
SHA-256:	0A39DCA0020CF1A5E3B0800E546DD1206EDE363209971B09D98B260247005385
SHA-512:	87A2A3AF0E1C1FECB44019D08314503F137EADC00BCE0D550FFD8D6C4BB3BE6B4FB4C7528862ECB1D8E1C80647A8BF0DBDDFACF95EE60FAFD38DCFB29F3E7235
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... ....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\...x....Mj}9oE...7....*.....]..(...x..:.e...+..6..r.....#XP.Q^(.*uz.....G...V_.~....3.c.o.?g.....z.8...Q...9(.Z.'.C...U...5..+....)h...i)M.,c.%{$.....x..=.Yp..%5~...f?..... <.....GR.....:).d.....3/.H.....Z..+Z..|.7..A.m.c..;g...]..n..3.Ft..(.KI]&b.QE.&(.._.C.....B...-..h.Dh.....{..J*.qNN...Z.....?...../.H.v..O.|.....I"]Z.

C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe

Process:	C:\Users\user\Desktop\yIF7nMz573.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	366080
Entropy (8bit):	7.206487159159595
Encrypted:	false
SSDEEP:	6144:LSdUnaLFGk01lHybFuN0O4tCZa5bIBur00I1caYxjn+FPUBqVYehA:OmniGFlHOAN05tC6MBuQ0IQhn+FsBqak
MD5:	DCE2A8F4AB60879898A21AB451CAD63F
SHA1:	C889640843424E5EE1C6A7E31D25E3FA510B846B
SHA-256:	2BE50564951116CA5AC96158ABDB936B6D5BD35794330371131F4117223CDD26
SHA-512:	76CCDED319F6425843A60262013267A66CA3669D3BC8F42652B6CF11D46DA10598E3EC985606CB3A10701105D85B13A682F29E7A7EE8B9926278B00AA363ED49
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-\..i=..i=..i=...r..h=..wo..v=..wo...=..N...j=..i=...=..wo..V=..wo..h=.. wo..h=..Richi=.....PE..L...j..a.....q.....0....@.....t.....g.....(.....t..?.....P..... ...@.....text..... ..`.data....)q..0...8.....@....sez....K....`t.....R.....@....yasufo.J....pt.....T.....@....rsrc....?....t..@...V. .....@..@..... .....

C:\Users\user\AppData\Roaming\110809d565579c\cred.dll

Process:	C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	276
Entropy (8bit):	5.243580622568483
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+knlTamcXaoD:J0+oxBeRmR9etdzRxGezH0qlZma+
MD5:	ED87E93DB5A2DC3D25A0C9C4D6D91CDC
SHA1:	CBC46DC3804EAE9D2F6CDBE650B4AE817B26EDFD
SHA-256:	52268E5929FC4D2F0E2EB8D097AC90B136DF895FE5B5F91A38F34AFBD58A513A
SHA-512:	6A7D4BFC704249588544AC92C7E74AFFCE91886CF01D1BBE64A554B95BEBC3F3AC87DCB1403C899C77DF9D4457615F033ADA1D6832678D42A45EA416FF0A66E1
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 185.215.113.15 Port 80</address>.</body></html>.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.206487159159595

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	yIF7nMz573.exe
File size:	366080
MD5:	dce2a8f4ab60879898a21ab451cad63f
SHA1:	c889640843424e5ee1c6a7e31d25e3fa510b846b
SHA256:	2be50564951116ca5ac96158abdb936b6d5bd35794330371131f4117223cdd26
SHA512:	76ccded319f6425843a60262013267a66ca3669d3bc8f42652b6cf11d46da10598e3ec985606cb3a10701105d85b13a682f29e7a7ee8b9926278b00aa363ed49
SSDEEP:	6144:LSdUnaLFGk01lHybFuN0O4tCZa5bIBur00I1caYxjn+FPUBqVYehA:OmniGFlHOAN05tC6MBuQ0lQhn+FsBqak
TLSH:	8574BF10FA90C431F1F712F449BA9668B92E7AA1572494CF53D56AEE4738AE4FC3130B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....- \..i=..i=..i=...r..h=..wo..v=..wo...=..N...j=..i=...=..wo..V=..wo..h=..wo..h=..Richi=.....PE..L...j..a...

File Icon

Icon Hash:	aedaae9ecea62aa2

Static PE Info

General

Entrypoint:	0x40eec0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6104AC6A [Sat Jul 31 01:50:34 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	9708e7dbb84fb2e34dfb5e05eada89dd

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007F584475660Bh
call 00007F5844748F76h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 00430CA0h
push 00412510h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h
push ebx
push esi
push edi
mov eax, dword ptr [0045548Ch]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-70h], 00000000h
mov dword ptr [ebp-04h], 00000000h
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [004010DCh]
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007F5844748F88h
mov eax, 00000001h
ret
mov esp, dword ptr [ebp-18h]
mov dword ptr [ebp-78h], 000000FFh
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, dword ptr [ebp-78h]
jmp 00007F58447490B8h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007F58447490F4h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007F58447576CAh
add esp, 04h
test eax, eax
jne 00007F5844748F6Ch
push 0000001Ch
call 00007F58447490ACh
add esp, 04h
call 00007F5844750CF4h
test eax, eax
jne 00007F5844748F6Ch
push 00000010h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x313bc	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x748000	0x3f98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1350	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xb2f0	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x2fc	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x315ac	0x31600	False	0.4516465585443038	data	6.387563290024678	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x33000	0x7129a8	0x23800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.sez	0x746000	0x4b	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.yasufo	0x747000	0x4a	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x748000	0x3f98	0x4000	False	0.7305908203125	data	6.33601075142428	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7481f0	0x25a8	data	Korean	North Korea
RT_ICON	0x7481f0	0x25a8	data	Korean	South Korea
RT_ICON	0x74a798	0x10a8	data	Korean	North Korea
RT_ICON	0x74a798	0x10a8	data	Korean	South Korea
RT_STRING	0x74b918	0x42	data	Korean	North Korea
RT_STRING	0x74b918	0x42	data	Korean	South Korea
RT_STRING	0x74b960	0x4ae	data	Korean	North Korea
RT_STRING	0x74b960	0x4ae	data	Korean	South Korea
RT_STRING	0x74be10	0x188	data	Korean	North Korea
RT_STRING	0x74be10	0x188	data	Korean	South Korea
RT_ACCELERATOR	0x74b8a8	0x70	data	Korean	North Korea
RT_ACCELERATOR	0x74b8a8	0x70	data	Korean	South Korea
RT_ACCELERATOR	0x74b868	0x40	data	Korean	North Korea
RT_ACCELERATOR	0x74b868	0x40	data	Korean	South Korea
RT_GROUP_ICON	0x74b840	0x22	data	Korean	North Korea
RT_GROUP_ICON	0x74b840	0x22	data	Korean	South Korea

Imports

DLL	Import
KERNEL32.dll	DebugBreakProcess, FindFirstChangeNotificationW, GetNamedPipeHandleStateW, CreateIoCompletionPort, FillConsoleOutputCharacterW, DisableThreadLibraryCalls, TerminateProcess, GetProcessId, VerifyVersionInfoW, EnumDateFormatsW, FindNextFileW, CopyFileExA, BuildCommDCBAndTimeoutsA, VirtualUnlock, WriteProfileStringW, VerifyVersionInfoA, SetProcessPriorityBoost, GetDriveTypeW, FindFirstChangeNotificationA, GetFileType, DeleteFileA, FindNextVolumeMountPointA, OutputDebugStringA, ResetWriteWatch, WriteConsoleInputA, WriteConsoleInputW, GetConsoleTitleW, SetComputerNameExW, SetTimeZoneInformation, LoadLibraryA, GetSystemDirectoryA, GetDriveTypeA, GetShortPathNameW, ActivateActCtx, GetProfileSectionA, DeleteFileW, GetCommandLineW, InterlockedIncrement, AddRefActCtx, FindResourceA, FormatMessageA, GetModuleFileNameW, CreateJobObjectW, InitializeCriticalSection, SetFirmwareEnvironmentVariableW, GetDllDirectoryW, GetExitCodeThread, WritePrivateProfileStringW, GetConsoleAliasesLengthW, WriteProfileSectionW, AddAtomA, InterlockedDecrement, GetVersionExA, HeapSize, _hwrite, GetStartupInfoA, DisconnectNamedPipe, GetCPInfoExW, GetSystemWow64DirectoryW, GetPrivateProfileIntA, GetConsoleAliasExesW, DebugBreak, EndUpdateResourceW, SetLastError, InterlockedExchangeAdd, GetStringTypeExW, DeleteVolumeMountPointW, OpenFileMappingA, SetDefaultCommConfigW, lstrcpyA, TerminateThread, GetACP, _lwrite, GetQueuedCompletionStatus, GetNamedPipeHandleStateA, GetDiskFreeSpaceExW, RemoveVectoredExceptionHandler, WriteConsoleW, VirtualProtect, ReadConsoleOutputW, SetThreadContext, BuildCommDCBA, ReleaseActCtx, GetHandleInformation, WritePrivateProfileSectionW, DeleteCriticalSection, GetFileAttributesA, OpenWaitableTimerW, GetVolumePathNameW, SetConsoleMode, HeapSetInformation, SetComputerNameA, FindNextFileA, SetEvent, UnlockFile, GetProcAddress, DeleteTimerQueueTimer, CopyFileW, MoveFileA, GlobalAlloc, GetCommMask, SetFileShortNameA, GetFileAttributesW, FreeEnvironmentStringsW, GetProfileStringA, GetConsoleTitleA, SetComputerNameW, GetConsoleAliasesW, CreateMailslotA, EnumDateFormatsA, GetTimeZoneInformation, SetConsoleOutputCP, GetFileInformationByHandle, SetLocalTime, CallNamedPipeA, GetConsoleAliasExesLengthW, GetCurrentActCtx, OpenSemaphoreW, GetModuleHandleExA, LoadLibraryW, FoldStringW, GetTickCount, GetConsoleAliasesLengthA, GetLastError, LocalUnlock, GetFileTime, EnumResourceNamesW, OpenFileMappingW, UnhandledExceptionFilter, GetCompressedFileSizeW, GetThreadPriority, ReadConsoleA, AssignProcessToJobObject, Sleep, EnterCriticalSection, LeaveCriticalSection, RaiseException, RtlUnwind, GetCurrentProcess, SetUnhandledExceptionFilter, IsDebuggerPresent, WideCharToMultiByte, GetCommandLineA, HeapValidate, IsBadReadPtr, GetModuleHandleA, TlsGetValue, GetModuleHandleW, TlsAlloc, TlsSetValue, GetCurrentThreadId, TlsFree, GetStdHandle, WriteFile, OutputDebugStringW, ExitProcess, GetOEMCP, GetCPInfo, IsValidCodePage, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, GetEnvironmentStringsW, SetHandleCount, HeapDestroy, HeapCreate, HeapFree, VirtualFree, FlushFileBuffers, GetConsoleCP, GetConsoleMode, HeapAlloc, HeapReAlloc, VirtualAlloc, InitializeCriticalSectionAndSpinCount, MultiByteToWideChar, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, LCMapStringA, LCMapStringW, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, SetFilePointer, CloseHandle, CreateFileA

Possible Origin

Language of compilation system	Country where language is spoken	Map
Korean	North Korea	
Korean	South Korea	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.215.113.1549746802027700 06/26/22-09:46:57.610393	TCP	2027700	ET TROJAN Amadey CnC Check-In	49746	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549749802027700 06/26/22-09:47:01.350218	TCP	2027700	ET TROJAN Amadey CnC Check-In	49749	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549798802027700 06/26/22-09:47:41.864054	TCP	2027700	ET TROJAN Amadey CnC Check-In	49798	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549832802027700 06/26/22-09:48:33.213243	TCP	2027700	ET TROJAN Amadey CnC Check-In	49832	80	192.168.2.3	185.215.113.15

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.215.113.1549755802027700 06/26/22-09:47:21.773924	TCP	2027700	ET TROJAN Amadey CnC Check-In	49755	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549826802027700 06/26/22-09:48:24.530301	TCP	2027700	ET TROJAN Amadey CnC Check-In	49826	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549829802027700 06/26/22-09:48:27.114493	TCP	2027700	ET TROJAN Amadey CnC Check-In	49829	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549841802027700 06/26/22-09:48:43.294919	TCP	2027700	ET TROJAN Amadey CnC Check-In	49841	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549780802027700 06/26/22-09:47:27.628822	TCP	2027700	ET TROJAN Amadey CnC Check-In	49780	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549767802027700 06/26/22-09:47:22.040844	TCP	2027700	ET TROJAN Amadey CnC Check-In	49767	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549761802027700 06/26/22-09:47:20.297421	TCP	2027700	ET TROJAN Amadey CnC Check-In	49761	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549801802027700 06/26/22-09:47:44.118576	TCP	2027700	ET TROJAN Amadey CnC Check-In	49801	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549776802027700 06/26/22-09:47:25.997227	TCP	2027700	ET TROJAN Amadey CnC Check-In	49776	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549810802027700 06/26/22-09:47:57.512185	TCP	2027700	ET TROJAN Amadey CnC Check-In	49810	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549773802027700 06/26/22-09:47:23.164370	TCP	2027700	ET TROJAN Amadey CnC Check-In	49773	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549758802027700 06/26/22-09:47:18.795200	TCP	2027700	ET TROJAN Amadey CnC Check-In	49758	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549782802027700 06/26/22-09:47:29.252532	TCP	2027700	ET TROJAN Amadey CnC Check-In	49782	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549756802027700 06/26/22-09:47:13.646635	TCP	2027700	ET TROJAN Amadey CnC Check-In	49756	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549785802027700 06/26/22-09:47:30.265752	TCP	2027700	ET TROJAN Amadey CnC Check-In	49785	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549828802027700 06/26/22-09:48:25.611929	TCP	2027700	ET TROJAN Amadey CnC Check-In	49828	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549816802027700 06/26/22-09:48:09.646530	TCP	2027700	ET TROJAN Amadey CnC Check-In	49816	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549845802027700 06/26/22-09:48:46.784890	TCP	2027700	ET TROJAN Amadey CnC Check-In	49845	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549774802027700 06/26/22-09:47:24.256337	TCP	2027700	ET TROJAN Amadey CnC Check-In	49774	80	192.168.2.3	185.215.113.15

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.215.113.1549839802027700 06/26/22-09:48:37.748469	TCP	2027700	ET TROJAN Amadey CnC Check-In	49839	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549797802027700 06/26/22-09:47:41.469763	TCP	2027700	ET TROJAN Amadey CnC Check-In	49797	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549817802027700 06/26/22-09:48:11.724189	TCP	2027700	ET TROJAN Amadey CnC Check-In	49817	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549786802027700 06/26/22-09:47:30.623905	TCP	2027700	ET TROJAN Amadey CnC Check-In	49786	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549745802027700 06/26/22-09:46:54.779771	TCP	2027700	ET TROJAN Amadey CnC Check-In	49745	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549757802027700 06/26/22-09:47:16.401762	TCP	2027700	ET TROJAN Amadey CnC Check-In	49757	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549823802027700 06/26/22-09:48:17.269325	TCP	2027700	ET TROJAN Amadey CnC Check-In	49823	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549751802027700 06/26/22-09:47:05.409898	TCP	2027700	ET TROJAN Amadey CnC Check-In	49751	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549781802027700 06/26/22-09:47:28.674122	TCP	2027700	ET TROJAN Amadey CnC Check-In	49781	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549805802027700 06/26/22-09:47:48.812945	TCP	2027700	ET TROJAN Amadey CnC Check-In	49805	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549775802027700 06/26/22-09:47:25.180668	TCP	2027700	ET TROJAN Amadey CnC Check-In	49775	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549803802027700 06/26/22-09:47:47.323846	TCP	2027700	ET TROJAN Amadey CnC Check-In	49803	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549812802027700 06/26/22-09:47:59.897990	TCP	2027700	ET TROJAN Amadey CnC Check-In	49812	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549806802027700 06/26/22-09:47:54.097536	TCP	2027700	ET TROJAN Amadey CnC Check-In	49806	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549784802027700 06/26/22-09:47:30.001407	TCP	2027700	ET TROJAN Amadey CnC Check-In	49784	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549787802027700 06/26/22-09:47:30.877538	TCP	2027700	ET TROJAN Amadey CnC Check-In	49787	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549793802027700 06/26/22-09:47:39.471421	TCP	2027700	ET TROJAN Amadey CnC Check-In	49793	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549796802027700 06/26/22-09:47:40.783332	TCP	2027700	ET TROJAN Amadey CnC Check-In	49796	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549799802027700 06/26/22-09:47:42.867694	TCP	2027700	ET TROJAN Amadey CnC Check-In	49799	80	192.168.2.3	185.215.113.15

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.215.113.1549830802027700 06/26/22-09:48:30.483127	TCP	2027700	ET TROJAN Amadey CnC Check-In	49830	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549818802027700 06/26/22-09:48:13.810900	TCP	2027700	ET TROJAN Amadey CnC Check-In	49818	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549744802027700 06/26/22-09:46:53.237130	TCP	2027700	ET TROJAN Amadey CnC Check-In	49744	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549815802027700 06/26/22-09:48:05.618223	TCP	2027700	ET TROJAN Amadey CnC Check-In	49815	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549842802027700 06/26/22-09:48:44.262889	TCP	2027700	ET TROJAN Amadey CnC Check-In	49842	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549791802027700 06/26/22-09:47:37.619364	TCP	2027700	ET TROJAN Amadey CnC Check-In	49791	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549824802027700 06/26/22-09:48:18.293793	TCP	2027700	ET TROJAN Amadey CnC Check-In	49824	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549833802027700 06/26/22-09:48:36.596810	TCP	2027700	ET TROJAN Amadey CnC Check-In	49833	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549750802027700 06/26/22-09:47:03.761613	TCP	2027700	ET TROJAN Amadey CnC Check-In	49750	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549809802027700 06/26/22-09:47:55.667044	TCP	2027700	ET TROJAN Amadey CnC Check-In	49809	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549825802027700 06/26/22-09:48:19.702891	TCP	2027700	ET TROJAN Amadey CnC Check-In	49825	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549788802027700 06/26/22-09:47:31.215612	TCP	2027700	ET TROJAN Amadey CnC Check-In	49788	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549794802027700 06/26/22-09:47:42.618057	TCP	2027700	ET TROJAN Amadey CnC Check-In	49794	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549753802027700 06/26/22-09:47:07.860735	TCP	2027700	ET TROJAN Amadey CnC Check-In	49753	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549747802027700 06/26/22-09:46:59.493020	TCP	2027700	ET TROJAN Amadey CnC Check-In	49747	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549813802027700 06/26/22-09:48:02.729973	TCP	2027700	ET TROJAN Amadey CnC Check-In	49813	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549765802027700 06/26/22-09:47:21.494001	TCP	2027700	ET TROJAN Amadey CnC Check-In	49765	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549742802027700 06/26/22-09:46:52.260106	TCP	2027700	ET TROJAN Amadey CnC Check-In	49742	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549777802027700 06/26/22-09:47:26.632947	TCP	2027700	ET TROJAN Amadey CnC Check-In	49777	80	192.168.2.3	185.215.113.15

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3185.215.113.1549783802027700 06/26/22-09:47:29.721183	TCP	2027700	ET TROJAN Amadey CnC Check-In	49783	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549790802027700 06/26/22-09:47:31.866868	TCP	2027700	ET TROJAN Amadey CnC Check-In	49790	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549802802027700 06/26/22-09:47:45.689140	TCP	2027700	ET TROJAN Amadey CnC Check-In	49802	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549789802027700 06/26/22-09:47:31.596641	TCP	2027700	ET TROJAN Amadey CnC Check-In	49789	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549754802027700 06/26/22-09:47:11.567118	TCP	2027700	ET TROJAN Amadey CnC Check-In	49754	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549795802027700 06/26/22-09:47:39.970739	TCP	2027700	ET TROJAN Amadey CnC Check-In	49795	80	192.168.2.3	185.215.113.15
192.168.2.3185.215.113.1549820802027700 06/26/22-09:48:15.889921	TCP	2027700	ET TROJAN Amadey CnC Check-In	49820	80	192.168.2.3	185.215.113.15

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:46:52.202889919 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:52.204113007 CEST	49743	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:52.259402037 CEST	80	49742	185.215.113.15	192.168.2.3
Jun 26, 2022 09:46:52.259541035 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:52.260106087 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:52.263921022 CEST	80	49743	185.215.113.15	192.168.2.3
Jun 26, 2022 09:46:52.264056921 CEST	49743	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:52.264534950 CEST	49743	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:52.322077990 CEST	80	49742	185.215.113.15	192.168.2.3
Jun 26, 2022 09:46:52.333787918 CEST	80	49743	185.215.113.15	192.168.2.3
Jun 26, 2022 09:46:53.021445990 CEST	80	49742	185.215.113.15	192.168.2.3
Jun 26, 2022 09:46:53.021548033 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.022270918 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.022458076 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.022586107 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.022691011 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.022790909 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.022902966 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023004055 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023108959 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023211002 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023314953 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023422003 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023520947 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023627043 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023758888 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023874044 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.023931026 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.024036884 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.024138927 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.024267912 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.024373055 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.024490118 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.024573088 CEST	49742	80	192.168.2.3	185.215.113.15

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:46:53.024672985 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.024806976 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.024982929 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.025115013 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.025243044 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.025348902 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.025456905 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.025561094 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.025659084 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.025764942 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.025861025 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.025962114 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026062012 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026165962 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026271105 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026367903 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026465893 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026567936 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026669025 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026767969 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026873112 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.026971102 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027086973 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027179003 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027282000 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027385950 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027482986 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027589083 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027690887 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027793884 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027894974 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.027997017 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.028109074 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.028213024 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.028321981 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.028424978 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.028526068 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.028631926 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.028734922 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.028840065 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.028939962 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029043913 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029146910 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029251099 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029352903 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029460907 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029566050 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029668093 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029772043 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029877901 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.029978037 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.030086040 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.030190945 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.030294895 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.030400038 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.030508041 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.030616045 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.030718088 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.030821085 CEST	49742	80	192.168.2.3	185.215.113.15

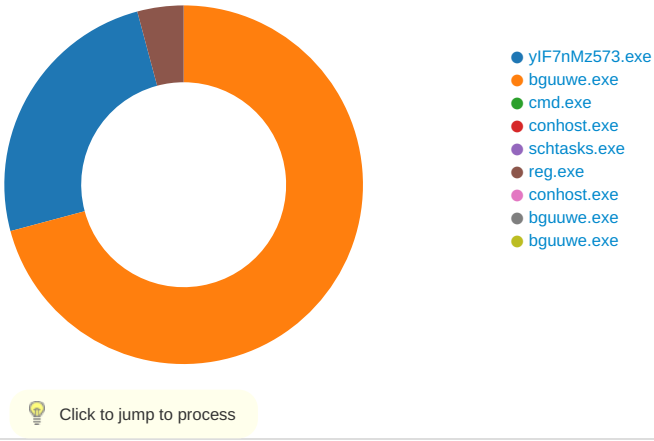
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 26, 2022 09:46:53.030942917 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.031053066 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.031188011 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.031297922 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.031431913 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.031591892 CEST	49742	80	192.168.2.3	185.215.113.15
Jun 26, 2022 09:46:53.031721115 CEST	49742	80	192.168.2.3	185.215.113.15

HTTP Request Dependency Graph

- 185.215.113.15

Statistics

Behavior



System Behavior

Analysis Process: yIF7nMz573.exe PID: **6472**, Parent PID: **4804**

General

Target ID:	0
Start time:	09:46:40
Start date:	26/06/2022
Path:	C:\Users\user\Desktop\yIF7nMz573.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\yIF7nMz573.exe"
Imagebase:	0x400000
File size:	366080 bytes
MD5 hash:	DCE2A8F4AB60879898A21AB451CAD63F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: bguuwe.exe PID: **6608**, Parent PID: **6472**

General

Target ID:	1
Start time:	09:46:46
Start date:	26/06/2022
Path:	C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe"
Imagebase:	0x400000
File size:	366080 bytes
MD5 hash:	DCE2A8F4AB60879898A21AB451CAD63F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 46%, ReversingLabs
Reputation:	low

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	409423	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409423	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409423	HttpSendRequestA
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	409423	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409423	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409423	HttpSendRequestA
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	409423	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409423	HttpSendRequestA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409423	HttpSendRequestA
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	409423	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409423	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409423	HttpSendRequestA
C:\Users\user\AppData\Roaming\110809d565579c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	410A0F	CreateDirectoryA
C:\Users\user\AppData\Roaming\110809d565579c\cred.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	408365	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\425620883392	success or wait	14	420A63	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\110809d565579c\cred.dll	0	276	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 31 38 35 2e 32 31 35 2e 31 31 33 2e 31 35 20 50 6f 72 74 20 38 30 3c 2f 61 64 64	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html> <head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.41 (Ubuntu) Server at 185.215.113.15 Port 80</add	success or wait	1	4083CA	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\425620883392	unknown	4	success or wait	99843	408DD4	ReadFile

Analysis Process: cmd.exe PID: **6764**, Parent PID: **6608**

General	
Target ID:	4
Start time:	09:46:50
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\Users\user\AppData\Local\Temp\62eca45584\
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
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: **6776**, Parent PID: **6764**

General	
Target ID:	5
Start time:	09:46:51
Start date:	26/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **6784**, Parent PID: **6608**

General	
Target ID:	6
Start time:	09:46:51
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN bguuwe.exe /TR "C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe" /F
Imagebase:	0x13c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
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: reg.exe PID: **6816**, Parent PID: **6764**

General

Target ID:	7
Start time:	09:46:51
Start date:	26/06/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\Users\user\AppData\Local\Temp\62eca45584\
Imagebase:	0x330000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
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

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Startup	unicode	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	C:\Users\user\AppData\Local\Temp\62eca45584\	success or wait	1	335A1D	RegSetValueExW

Analysis Process: conhost.exe PID: **6832**, Parent PID: **6784**

General

Target ID:	8
Start time:	09:46:51
Start date:	26/06/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: bguuwe.exe PID: **6960**, Parent PID: **848**

General	
Target ID:	10
Start time:	09:46:53
Start date:	26/06/2022
Path:	C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe
Imagebase:	0x400000
File size:	366080 bytes
MD5 hash:	DCE2A8F4AB60879898A21AB451CAD63F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: bguuwe.exe PID: **6504**, Parent PID: **848**

General	
Target ID:	19
Start time:	09:48:00
Start date:	26/06/2022
Path:	C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\62eca45584\bguuwe.exe
Imagebase:	0x400000
File size:	366080 bytes
MD5 hash:	DCE2A8F4AB60879898A21AB451CAD63F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly