National Cyber Security Centre

a part of GCHQ

Indicators of Compromise for Malware used by APT28

4 October 2018

Introduction

Advanced Persistent Threat group, APT28 (also known as Fancy Bear, Pawn Storm, the Sednit Gang and Sofacy), is a highly skilled threat actor, best known for its disruptive cyber activity against the US Democratic National Committee (DNC) and the French channel TV5 Monde.

According to publicly available information, APT28 has previously used tools including X-Tunnel, X-Agent and CompuTrace to penetrate target networks. These tools can be used to hook into system drivers and access local passwords and the LDAP server. Reported capabilities include monitoring keystrokes and mouse movements, accessing webcams and USB drives, searching and replacing local files and maintaining a persistent connection.

The signatures and Indicators of Compromise (IoCs) included in this advisory will assist in detecting APT28 malware. Network based signatures alone will not guarantee successful identification of APT28 in a network. Many of the communication modules used by the actor are wrapped in protocols such as SSL/TLS, with the intention of evading content-based signatures.

Please use the indicators in this NCSC advisory to check for the presence of this malware on your platforms and networks.

Detecting known ATP28 tools

X-AGENT

X-AGENT (Also known as CHOPSTICK) is a second-stage modular remote access trojan (RAT). It can run on Windows, iOS and Unix-based operating systems.

Functions of X-AGENT include key logging and file extraction. It is often used after first stage malware such as CORESHELL or GAMEFISH. X-AGENT is likely to be used in conjunction with XTUNNEL and CompuTrace/Lojack**.** Recent versions of X-AGENT use SSL/TLS to encrypt the communications.

Indicators of Compromise (IoCs)

The following IP addresses and domains have been used for X-AGENT Command and Control (C2) servers, to communicate with victims:

IP Address	Domain
139.5.177.205	malaytravelgroup.com
80.255.6.15	worldimagebucket.com
89.34.111.107	fundseats.com
86.106.131.229	globaltechengineers.org
139.5.177.206	
185.181.102.203	beststreammusic.com
185.181.102.204	thepiratecinemaclub.org
169.239.129.31	coindmarket.com

213.252.247.112	creekcounty.net
185.86.148.15	
89.45.67.110	virtsvc.com
185.86.150.205	
193.37.255.10	moderntips.org
195.12.50.171	daysheduler.org
51.38.128.110	escochart.com
185.144.83.124	loungecinemaclub.com
185.216.35.10	genericnetworkaddress.com
185.94.192.122	bulgariatripholidays.com
185.216.35.7	georgia-travel.org
103.253.41.124	bbcweather.org
185.189.112.195	politicweekend.com
185.230.124.246	truefashionnews.com
87.120.254.106	protonhardstorage.com
77.81.98.122	moldtravelgroup.com
89.34.111.132	iboxmit.com
46.21.147.55	brownvelocity.org
103.208.86.57	pointtk.com
185.128.24.104	narrowpass.net
145.239.67.8	powernoderesources.com
185.210.219.250	
86.105.9.174	topcinemaclub.com
89.34.111.107	fundseats.com

Snort Rules

The following snort rules can be used to detect X-Agent communications between Command and Control (C2) servers and victims:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (flow:
established,from_client; msg: "XAgent Beacon"; content:
"HTTP/1.1|0d 0a|Accept|3a|
text/html,application/xhtml+xml,application/xml|3b|q=0.9,*";
!"Host|3a| yandex.ru";; pcre: "/^(?:GET|POST)
\/(?:watch|search|find|results|open|search|close)\/\?(?:text=|from
=|aq=|ai=|ags=|oe=|btnG=|oprnd=|utm=|channel=|itwm=)/";)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (flow:
established,from_client; msg:: "XAgent itwm beacon v1"; content:
"/?itwm"; fast_pattern; pcre: "/itwm=[A-Za-z0-9\-\_]{29,35}/";)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (flow:
established,from_client; msg:: "XAgent itwm beacon v2"; content:
"&itwm"; fast_pattern; pcre: "/&itwm=[A-Za-z0-9\-\_]{29,35}/";)
```

Hashes

The following are SHA-1 hashes of X-Agent files used by APT28:

Filename	Hash
chost.exe	46e2957e699fae6de1a212dd98ba4e2bb969497d
msoutlook.dll	c53930772beb2779d932655d6c3de5548810af3d
Samp_(16).file	fa695e88c87843ca0ba9fc04b176899ff90e9ac5
outlook.dll	046a8adc2ef0f68107e96babc59f41b6f0a57803

CompuTrace

CompuTrace/Lojack is a legitimate piece of software, which can track and assist in the recovery of lost or stolen laptops as well as remotely locking and deleting files.

APT28 have modified this software. Exploitation of this software enables persistence on the victim's operating system, as well as the ability to modify the system memory and retrieve additional modules through the installed modified CompuTrace/Lojack agent.

Indicators of Compromise (IoCs)

The following IP addresses have been used as Command and Control (C2) servers for APT28 LoJack communications:

IP Address
185.86.151.2
46.21.147.76
46.21.147.71
162.208.10.66
185.86.151.104
185.86.149.116
86.106.131.54
185.181.102.201
179.43.158.20
85.204.124.77
185.86.148.184
185.183.107.40
185.94.191.65
94.177.12.150
54.37.104.106
93.113.131.103
169.239.129.121
169.239.128.133

Snort Rules

The following snort rule can be used to detect CompuTrace communications from victims:

Please note: *The Snort rule provided may detect false positives due to CompuTrace/Lojack being legitimate software. The NCSC highly recommend* *network administrators assess their environment for the presence of CompuTrace/Lojack and adjust the signatures accordingly* to exclude the legitimate use of CompuTrace.

```
alert tcp any any <> any any (flow: established; msg: "APT28 -
CompuTrace_Beacon_UserAgent"; content: "|0d0a|TagId|3a| ";
fast_pattern; content: "POST / "; content:!"namequery.com";
content:!"Host: 209.53.113."; content:!"dnssearch.org";
content:!"Cookie:"; content:!"fnbcorporate.co.za";
content:!"207.6.98."; pcre: "/Mozilla\/[0-9]{1,2}.[0-9]{1,2}
\(compatible\; MSIE [0-9]{1,2}.[0-9]{1,2}\;\)\x0d\x0a/";)
```

Hashes

The following is a SHA-1 hash of a CompuTrace file used by APT28:

Filename	Hash
dcbfd12321fa7c4fa9a72486ced578fdc00dcee79e6d95aa481791f044a55dll	d70db6a6d660aae58ccfc688a2890391fd873bfb

XTUNNEL

X-TUNNEL (XTUNNEL) is a network tunnelling tool that is used for network traversal and pivoting. It provides a secure tunnel to an external command and control server, through which the actors can operate using a variety of standard networking tools and protocols to connect to internal services.

Indicators of Compromise (IoCs)

The following IP addresses and domains have been used for XTUNNEL communications

IP Address	Domain
23.163.0.59	picturecrawling.com
86.105.1.123	
185.86.149.218	
185.145.128.80	
89.37.226.106	
94.177.12.238	

Hashes

The following are MD5 hashes of XTUNNEL files:

Filename	Hash
gpu.dll	8dbe37dfb0d498f96fb7f1e09e9e5c8f
lncstnt.exe	5086989639aed17227b8d6b041ef3163

ZEBROCY

ZEBROCY is a tool used by APT28, which has been observed since late 2015. The communications module used by ZEBROCY transmits using HTTP. The implant has key logging and file exfiltration functionality and utilises a file collection capability that identifies files with particular extensions.

The primary deployment mechanism for ZEBROCY has been spear-phishing emails, in which the payload runs systeminfo, tasklist and also takes a screenshot.

Indicators of Compromise (IoCs)

The following IP addresses have been used for ZEBROCY victim communications:

IP Address
176.223.111.243
172.104.21.26
188.241.68.118
89.45.67.153
185.25.50.93
45.124.132.127

Snort Rules

The following snort rule can be used to detect a string present in ZEBROCY victim communications:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (flow:
established,from_client; msg: "APT28 - Web/request -FILE- content-
type"; content: "-FILE-"; pcre: "/[A-Z0-9\-]{16}-FILE-
[^\r\n]+.tmp/"
```

Hashes

The following are SHA-1 hashes of ZEBROCY files:

Filename	Hash
codexgigas_913ac13ff245baeff843a99dc2cbc1ff5f8c025c	913ac13ff245baeff843a99dc2cbc1ff5f8c025c
codexgigas_b758c7775d9bcdc0473fc2e738b32f05b464b175	b758c7775d9bcdc0473fc2e738b32f05b464b175

UpnP Error Handler	3e7dfe9a8d5955a825cb51cb6eec0cd07c569b41

Mitigation

Follow the high-level security mitigations detailed in the **NCSC mitigating malware guidance** (https://www.ncsc.gov.uk/guidance/mitigating-malware) and in the **Preventing Lateral Movement guidance** (https://www.ncsc.gov.uk/guidance/preventing-lateral-movement).

For additional mitigations for Windows 10 **follow the NCSC Windows 10 EUD guidance**: https://www.ncsc.gov.uk/guidance/eud-security-guidance-windows-10-1703. This guidance details how to configure AppLocker to help prevent malicious applications from running on end user devices.

Deploy SysMon. Microsoft SysInternals Tool SysMon, is able to monitor and log system activity to the Windows Event Log. It can provide information about process creations, network connections, and changes to file creation time.

By collecting the events it generates using Windows Event Collection or SIEM agents, and subsequently analysing them, Network Defenders and System Administrators can identify malicious or anomalous activity and understand how intruders and malware operate on their networks.

To help **reduce the risk of PowerShell being used as an attack vector** on the network, these two pieces of guidance will help:

- https://www.iad.gov/iad/library/ia-guidance/security-tips/powershell-security-risks-and-defenses.cfm
- https://www.asd.gov.au/publications/protect/securing-powershell.htm

Manage macros carefully:

- Disable Office macros except in the specific apps where they are required
- Only enable macros for users that need them day-to-day
- Ensure these users understand how harmful macros can be, and treat macros from untrusted sources with extreme caution
- Use a recent and fully patched version of Office.
- The underlying platform should, ideally, be configured in line with the NCSC's EUD Security Guidance. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/end-user-device-security and https://www.ncsc.gov.uk/guidance/macro-security-microsoft-office

Layer phishing defences. Detect and quarantine as many malicious email attachments and as much spam as possible, before they reach your end users. Multiple layers of defence will greatly cut the chances of a compromise.

- **Treat people as your first line of defence**. Tell staff how to report suspected phishing emails, and ensure they feel confident to do so. Investigate their reports promptly and thoroughly. Never punish users for clicking phishing links or opening attachments.

See NCSC Guidance: https://www.ncsc.gov.uk/phishing

Consider implementing a Security Information and Event Management (SIEM) solution to centrally collate logs from SysMon and Windows Event Logs.

Set up a security monitoring capability so you are collecting the data that will be needed to analyse network intrusions. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes