Malware Advisory

Alert: APT 10 Targeting UK Organizations

24th December, 2018

Table of Contents

Overview

APT10 (also known as Stone Panda, MenuPass and Red Apollo) is a threat actor known to have been active since at least 2009. Recently APT10 has compromised many global MSPs. The activity is global, but there is a significant UK impact. Industry information indicates that the exploitation methods vary depending on the location targeted. While the impact of the actor's intrusions may not be immediately evident, the loss of intellectual property and associated financial cost in the case of successful data theft can be considerable. A successful compromise may also result in significant penalties under GDPR, as APT10 have been observed in multiple cases exfiltration large volumes of personal data. And the organization itself is not at risk in isolation: infections can and do spread rapidly onward to infect its customers and/or supply chain.

This report is an update to the series of malware advisories focusing on MSP attacks. The Advisory released by us in October was emphasizing on the possible TTPs used by the APT10 to attack MSPs and the advisory released in December mentioned the compromised global MSPs. In this report new IOCs are there.

Severity: Severe
Release Date: 24th December, 2018
Target OS: Managed Service Providers
Distribution Method: Via vulnerability exploitation and Trojan installation
Discovered By: National Cyber Security Centre

Technical detail

a. How does it enters to the system

According to NCSC the malware APT10 is using for the compromise of MSPs is Quasar RAT. Quasar RAT, a publicly available remote administration tool known to use since 2017.

It's been observed that APT10 is deploying Quasar RAT in two components: one is to decrypt the payload and the other is to install the RAT as a service. FireEye named these components DILLJUICE and DILLWEED respectively.

In some cases APT10 has also used the certutil command to decode data and the psping command to check connectivity: both of these are common techniques used by red teams and attack groups.

In both cases the loader component for the malware searches through disk for an AES encrypted payload and attempts to decrypt then load it as a .NET assembly. The RAT then creates a unique mutex and contacts a command and control server via port 443. After initial infection, the actor try to either exfiltrate the data or deploy the cryptominer.

b. Technique used to enter your system

Initial infection

Industry data indicates that the actor is using phishing attacks to deliver the pen-testing tool Cobalt Strike. In some cases the actor is using the free, unlicensed version of Cobalt Strike, which is noisier as compared to the licensed one and can be detected by the IDS/IPS products. If the actor is having access to the network then Quasar RAT is deployed else he will exploit known vulnerability in commercial web applications, to get the access to the internet-facing web server. This compromised web server is then used by the actor to proxy traffic into the organisation's internal network.

Post-compromise

After getting access to the network then the actor will compromise domain administrator credentials for the entire network. For post exploitation the actor is using PowerShell scripting language. At some places instances of the tool 'PS2EXE' have been observed, which converts PowerShell scripts to exe files. In some scenarios Golden Ticket technique is used to forge Kerberos 'ticket granting tickets: this enables to the actor to move laterally around a network without the need for authentication credentials.

Data exfiltration is possible but there is not indicators to confirm the action. In some cases the exfiltrated data has been left in the recycle bin as a .RAR file, or forensic evidence is found pointing to the creation of RAR files which have been deleted once exfiltration has been achieved.

In some scenarios the actor has deployed cryptomining software. The cryptomining software used does change over time via a control channel.

Indicators of Compromise:

C2 IP:

- 185.111.74.127
- 194.68.44.108
- 66.70.135.104
- 185.211.247.52
- 195.54.163.74
- 167.114.171.8
- 37.10.71.100

Cryptominer IP communicating on port 443:

- 176.31.117.82

IOCs for APT10's Japan-focused activity: available open source

- 95.128.168.227
- 91.235.129.180
- 193.70.125.186
- www.jadl-or.com

Network defenders can also monitor their networks for usage of the certutil and psping commands, for example:

certutil.exe -decode<logname>.log <logname>.log

psping -acceptuela -w 0 -n 1 185.111.74.127:443

Mitigation measures

If you cannot do all these things straight away, do what you can now and plan to complete the rest later on – it will all help.

- Use multi-factor authentication. MFA helps a lot to stop attackers accessing your accounts due to password loss or theft.
- Secure your high-value accounts. This means accounts that can have a significant impact on the operation of entire systems and environments. For instance,
- Accounts with privileged or admin access. Restricting attackers' ability to exploit these accounts, will greatly reduce how much harm they can do.
- Restrict intruders' ability to move freely around your systems and networks. Pay particular attention to vulnerable entry points eg third-party systems with onward access to your core network. During an incident, disable remote access from third-party systems until you are sure they are clean.
- Whitelist applications. If supported by your operating environment, consider whitelisting permitted applications. This will help prevent malicious applications from running.
- Use antivirus. Keep it up to date, use it to scan your networks regularly and consider use of a cloud-backed antivirus product. These provide better threat intelligence and more advanced analysis. Make sure your antivirus covers MS Office macros.
- Protect your devices and networks by keeping them up to date, as APT10 have been seen taking advantage of unpatched vulnerabilities. Use supported software versions (the most recent that you can), and apply security patches promptly.
- Log the right events, as this will help you to detect the attacks detailed in this advisory. You need to know what binaries are running on your desktop, and what IP addresses are connecting to the internet.
- If you are a customer of an MSP, contact them and make sure you are happy with what they tell you about how they are handling this situation.

Preventive Measures

An organization's ability to rapidly respond to and recover from an incident begins with the development of an incident response capability. An organization's response capability should focus on being prepared to handle the most common attack vectors (e.g., spearphishing, malicious web content, credential theft). In general, organizations should prepare by:

- Establishing and periodically updating an incident response plan.
- Establishing written guidelines that prioritize incidents based on mission impact, so that an appropriate response can be initiated.
- Developing procedures and out-of-band lines of communication to handle incident reporting for internal and external relationships.
- Exercising incident response measures for various intrusion scenarios regularly, as part of a training regime.
- Committing to an effort that secures the endpoint and network infrastructure: prevention is less costly and more effective than reacting after an incident.

References

- https://www.ncsc.gov.uk/alerts/apt10-continuing-target-uk-organisations