National Cyber Security Centre
a part of GCHQ

Alert: APT10 continues to target UK organisations across wide range of sectors

Version 2.0

Reference: NCSC-Ops/25-18

20 December 2018

Introduction

APT10 (also known as Stone Panda, MenuPass and Red Apollo) is a threat actor known to have been active since at least 2009. Since then it has targeted healthcare, defence, aerospace, government, heavy industry/mining, Managed Service Providers (MSPs) and IT industries, among many other sectors, for the likely purpose of intellectual property theft. In 2017 its targeting of several global MSPs, giving it extensive access to the networks of organisations worldwide, was widely reported by the NCSC and industry partners.[1]

The NCSC is aware of current malicious activity affecting UK organisations across a broad range of sectors, likely conducted by APT10. This activity will almost certainly have been facilitated by the group's targeting of MSPs, as well as other outsourcing providers.

This report is an update to Version 1.0, issued to the CiSP information sharing platform on 29 August 2018 with a handling caveat of TLP AMBER. There have been minor changes to the content of the report and the mitigation advice has been updated.

Details

Industry partners investigating this current activity have provided insights into the techniques used and indicators of compromise.

Impact

The activity is global, but there is a significant UK impact; open source reporting has also highlighted a focus on Japan.[2] 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 exfiltrating large volumes of personal data. And the organisation itself is not at risk in isolation: infections can and do spread rapidly onward to infect its customers and/or supply chain.

Malware

Industry data indicates that in the UK the actor has been principally using the malware Quasar RAT, a publicly available remote administration tool that APT10 has been

[1] https://www.ncsc.gov.uk/information/global-targeting-enterprises-managed-service-providers, https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html

[2] https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

known to use since 2017. This currently appears to be more prevalent in the UK than the RedLeaves and PlugX malware that have also previously been used by APT10.

The actor has been observed deploying Quasar RAT in two components: one to decrypt the payload and the other to install the RAT as a service. FireEye name these components DILLJUICE and DILLWEED respectively.

In some cases the actor 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, and have been used by APT10 in the past.

Industry partners have reported that the deployment of Quasar RAT in the current activity correlates with previously reported APT10 techniques.[3] 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 (see associated IPs below).

Tools and techniques

Initial infection

In most instances Quasar RAT is deployed on a network to which the actor already has access, usually as a result of moving laterally from the network of a company's MSP or another supplier.

However, when it does not already have access via a compromised supplier, industry partners note that in some cases the actor has exploited known vulnerabilities in commercial web applications, giving it access to an internet-facing web server. This web server is then used to proxy traffic into the organisation's internal network.

Industry data also indicates that the actor using phishing attacks to deliver the pen-testing tool Cobalt Strike. In some cases the actor has been observed using the free, unlicensed version of Cobalt Strike, which is relatively noisy and can be detected by many intrusion detection products. While industry data suggests the use of Cobalt Strike has primarily been focused on Japan rather than the UK, the tool is widely deployed here by other cyber actors.

Post-compromise

When access to a network is achieved, industry partners have noted that the actor commonly compromises domain administration credentials for the entire network, enabling it to have widespread illegitimate access through legitimate means. The actor has been observed in some cases accessing MSP networks or systems in geographic locations where customer-facing IT service desks and support functions are based.

Post-compromise, the actor has also been observed using the scripting language PowerShell. Industry partners have seen instances of the tool 'PS2EXE', which converts PowerShell scripts to exe files. They also report the use in more mature intrusions of the Golden Ticket technique to forge Kerberos 'ticket granting tickets'

[3] https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html

(TGTs): this enables to the actor to move laterally around a network without the need for authentication credentials.

There is evidence that the actor seeks to use its access to exfiltrate data, although it is not always possible to determine whether it is successful. Industry partners have reported that data exfiltrated often relates to human resources information, suggesting an interest in the targeted company specifically, as well as potentially developing access to customers and suppliers. 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.

Industry partners have observed a time-lag, often of around seven days, between the actor's initial access to the network and any follow-on exploitation activities. One possible explanation for this is that the access and exploitation efforts are carried out by different 'teams' within the threat group.

The actor has also been observed in some cases deploying cryptomining software, likely as a tactic to distract network administrators and incident responses teams from the RAT activity. The cryptomining software used does change over time via a control channel although the exact reasons for this are unclear.

Indicators of compromise

NCSC and industry analysis has identified new IP addresses associated with this likely APT10 activity. The following are likely C2 IPs and can be used for scanning or monitoring, to detect potential APT10 activity on a network:

- 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

In cases when a cryptominer was seen on a network, industry partners report communication between the cryptominer and the following IP address over port 443:

- 176.31.117.82

The following IOCs for APT10's Japan-focused activity have also been provided in open source, although NCSC is unable to verify their validity.[4]

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

[4] https://www.lac.co.jp/lacwatch/people/20180521_001638.html

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

It is worth noting that both commands are legitimate utilities and therefore their usage is not necessarily indicative of malicious activity. For more information on how to log and query events on your network, see the mitigation advice at the end of this report.

Network defenders are also advised to search their recycle bins for evidence of .RAR files that may indicate exfiltrated data.

Conclusion

APT10 remains a significant and widespread threat to UK organisations of all sizes and affiliations. Its successful targeting of MSPs in recent years has afforded it a means to access networks globally on a vast scale.

Nonetheless, the targeting methods used are not highly sophisticated and in many cases their impact can be mitigated through the implementation of basic security measures. Network defenders are advised to investigate and monitor their networks for the indicators provided and to follow the mitigation advice below. If evidence of malicious activity is found on an organisation's network, full investigation and remediation is strongly advised, with guidance from an experienced Cyber Incident Response company.[5]

[5] For more information see https://www.ncsc.gov.uk/scheme/cyber-incidents

Mitigation

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. See NCSC guidance: https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services
- **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. See NCSC Guidance and Blogs: https://www.ncsc.gov.uk/guidance/systems-administration-architectures https://www.ncsc.gov.uk/blog-post/protecting-system-administration-pam https://www.ncsc.gov.uk/blog-post/protect-your-management-interfaces
  If you are securing a Windows estate, read this Microsoft recommended guidance too: https://docs.microsoft.com/en-gb/windows-server/identity/securing-privileged-access/securing-privileged-access
- **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. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/preventing-lateralmovement and https://www.ncsc.gov.uk/guidance/assessing-supply-chain-security
- **Whitelist applications.** If supported by your operating environment, consider whitelisting permitted applications. This will help prevent malicious applications from running. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/eudsecurity-guidance-windows-10-1709#applicationwhitelistingsection
- **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. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/macro-security-microsoft-office and https://www.ncsc.gov.uk/guidance/mitigating-malware
- **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. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware
- **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 can't currently assess whether an IOC is on your network, applying this guidance will help you to work that out: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes
- **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. Here are some questions you should ask them: https://www.ncsc.gov.uk/information/global-targetingenterprises-managed-service-providers