APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat

fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

Breadcrumb

Threat Research

FireEye iSIGHT Intelligence

Apr 06, 2017

5 mins read

APT10 Background

APT10 (MenuPass Group) is a Chinese cyber espionage group that FireEye has tracked since 2009. They have historically targeted construction and engineering, aerospace, and telecom firms, and governments in the United States, Europe, and Japan. We believe that the targeting of these industries has been in support of Chinese national security goals, including acquiring valuable military and intelligence information as well as the theft of confidential business data to support Chinese corporations. PwC and BAE recently issued a joint blog detailing extensive APT10 activity.

APT10's Resurgence

In June 2016, FireEye iSIGHT intelligence first reported that APT10 expanded their operations. The group was initially detected targeting a Japanese university, and more widespread targeting in Japan was subsequently uncovered. Further collaboration between FireEye as a Service (FaaS), Mandiant and FireEye iSIGHT intelligence uncovered additional victims worldwide, a new suite of tools and novel techniques.

Global Targeting Using New Tools

Leveraging its global footprint, FireEye has detected APT10 activity across six continents in 2016 and 2017. APT10 has targeted or compromised manufacturing companies in India, Japan and Northern Europe; a mining company in South America; and multiple IT service providers worldwide. We believe these companies are a mix of final targets and organizations that could provide a foothold in a final target.

APT10 unveiled new tools in its 2016/2017 activity. In addition to the continued use of SOGU, the current wave of intrusions has involved new tools we believe are unique to APT10. HAYMAKER and SNUGRIDE have been used as first stage backdoors, while BUGJUICE and a customized version of the open source QUASARRAT have been used as second stage backdoors. These new pieces of malware show that APT10 is devoting resources to capability development and innovation.

- HAYMAKER is a backdoor that can download and execute additional payloads in the form of modules. It also conducts basic victim profiling activity, collecting the computer name, running process IDs, %TEMP% directory path and version of Internet Explorer. It communicates encoded system information to a single hard coded command and control (C2) server, using the system's default User-Agent string.
- BUGJUICE is a backdoor that is executed by launching a benign file and then hijacking the search order to load a malicious dll into it. That malicious dll then loads encrypted shellcode from the binary, which is decrypted and runs the final BUGJUICE payload. BUGJUICE defaults to TCP using a custom binary protocol to communicate with the C2, but can also use HTTP and HTTPs if directed by the C2. It has the capability to find files, enumerate drives, exfiltrate data, take screenshots and provide a reverse shell.

- SNUGRIDE is a backdoor that communicates with its C2 server through HTTP requests. Messages are encrypted using AES with a static key. The malware's capabilities include taking a system survey, access to the filesystem, executing commands and a reverse shell. Persistence is maintained through a Run registry key.
- QUASARRAT is an open-source RAT available here. The versions used by APT10 (1.3.4.0, 2.0.0.0, and 2.0.0.1) are not available via the public GitHub page, indicating that APT10 has further customized the open source version. The 2.0 versions require a dropper to decipher and launch the AES encrypted QUASARRAT payload. QUASARRAT is a fully functional .NET backdoor that has been used by multiple cyber espionage groups in the past.

Traditional and Novel Methods

This recent APT10 activity has included both traditional spear phishing and access to victim's networks through service providers. (For more information on infection via service providers see M-Trends 2016). APT10 spear phishes have been relatively unsophisticated, leveraging .lnk files within archives, files with double extensions (e.g. "[Redacted]_Group_Meeting_Document_20170222_doc_.exe) and in some cases simply identically named decoy documents and malicious launchers within the same archive.

In addition to the spear phishes, FireEye ISIGHT Intelligence has observed APT10 accessing victims through global service providers. Service providers have significant access to customer networks, enabling an attacker who had compromised a service provider to move laterally into the network of the service provider's customer. In addition, web traffic between a service provider's customer and a service provider is likely to be viewed as benign by network defenders at the customer, allowing the attacker to exfiltrate data stealthily. A notable instance of this observed by FireEye involved a SOGU backdoor that was set to communicate with its C2 through a server belonging to the victim's service provider.

APT10 actors issued the following commands to a SOGU implant at a victim:

- sc create CorWrTool binPath= "\"C:\Windows\vss\vixDiskMountServer.exe\"" start= auto displayname= "Corel Writing Tools Utility" type= own
- sc description CorWrTool "Corel Graphics Corporation Applications."
- ping -a [Redacted]
- psexec.exe <orghost> d.exe
- net view /domain:[Redacted]
- proxyconnect - "port": 3389, "server": "[IP Address Redacted]"

These commands included setting persistence on the victim's system. The actor then tested connectivity to an IP managed by the victim's service provider. Once connectivity to the service provider IP was verified, the actor established the service provider IP as a proxy for the victim's SOGU backdoor. This effectively routes SOGU malware traffic through the

victim's service provider, which likely indicates a foothold on the service provider's network. The tactic also serves to mask malicious C2 and exfiltration traffic and make it appear innocuous.

Implications

APT10 is a threat to organizations worldwide. Their abuse of access to service provider networks demonstrates that peripheral organizations continue to be of interest to a malicious actor – especially those seeking alternative angles of attack. We believe the pace of APT10 operations may slow following the public disclosure by the PwC/BAE blog; however, we believe they will return to their large-scale operations, potentially employing new tactics, techniques and procedures.