ChessMaster Makes its Move: A Look into its Arsenal

blog.trendmicro.com/trendlabs-security-intelligence/chessmaster-cyber-espionage-campaign/

July 27, 2017

Malware

ChessMaster, a campaign targeting Japanese academe, technology enterprises, media outfits, managed service providers, and government agencies, employs malware-laden spear-phishing emails with decoy documents purporting to be legitimate.

By: Benson Sy, Kawabata Kohei July 27, 2017 Read time: (words)

From gathering intelligence, using the right social engineering lures, and exploiting vulnerabilities to laterally moving within the network, targeted attacks have multifarious tools at their disposal. And like in a game of chess, they are the set pieces that make up their modus operandi.

Take for instance the self-named ChessMaster, a campaign targeting Japanese academe, technology enterprises, media outfits, managed service providers, and government agencies. It employs various poisoned pawns in the form of malware-laden spear-phishing emails containing decoy documents. And beyond ChessMaster's endgame and pawns, we also found red flags that allude to its links to APT 10, also known as menuPass, POTASSIUM, Stone Panda, Red Apollo, and CVNX.

ChessMaster's name is from pieces of chess/checkers/draughts we found in the resource section of the main backdoor they use against their targets: ChChes, which Trend Micro detects as BKDR_CHCHES.

What makes the campaign unique is its arsenal of tools and techniques:

- ***Malicious shortcut (LNK) files and PowerShell.*** The LNK files execute Command Prompt that downloads a PowerShell script, which would either directly drop or reflectively load ChChes into the machine. The latter method makes ChChes a fileless malware.
- ***Self-extracting archive (SFX).*** An archive that drops an executable (EXE), a dynamic-link library (DLL), and a binary file (.BIN). Upon their extraction, malicious code is injected into the process of a legitimate file/application (DLL hijacking). ChessMaster takes it up a notch via load-time dynamic linking to trigger the malicious DLL's function.

- ***Runtime packers.*** Throughout its campaign, ChChes used three packers to obfuscate itself and avoid detection. The first had no encryption and a varied loader code. The second had a buggy (or anti-emulation) exclusive OR (XOR) encryption technique. The third added an AES algorithm on top of XOR encryption. Their compile dates overlap, which indicates ChChes' authors take cues and fine-tune their malware.
- ***Second-stage payloads.*** Additional malware are introduced to the infected system for persistence. These are actually variants of ChChes that use similar entry points but different and encrypted C&C communication.
- ***Hacking Tools.*** ChessMaster draws on legitimate email and browser password recovery and dumping tools they've misused and modified for their campaign. These can restore forgotten passwords, which are then dumped and retrieved. Lateral movement and further attacks can be worked out from here.
- ***TinyX.*** A version of PlugX sans the plug-in functionality that allows it to adopt new capabilities. TinyX is bundled separately in spear-phishing emails.
- ***RedLeaves.*** A second-stage backdoor that operates like the open-source and fileless remote access Trojan (RAT) Trochilus, which is known for enabling lateral movement in the infected systems. RedLeaves adopted capabilities from PlugX. In April, a RedLeaves variant named *himawari* (Japanese for sunflower) emerged capable of evading YARA rules released during that time.

ChessMaster and APT 10 Plays the Same Cyberespionage Game

APT 10/menuPass is a cyberespionage group whose specific campaign, Operation Cloud Hopper, attacked the intermediaries of their targets of interest—managed service providers (MSPs). Its notoriety stems from their prolific use of multifarious information-stealing backdoors and vulnerability exploits, along with the tenacity of its subterfuges, from spear-phishing emails to attack and infection chains. It also abused legitimate or open-source remote administration tools to steal data.

If that sounded familiar, it's because ChessMaster and APT 10 appear to be playing the same cyberespionage game. Here's a further illustration:

Figure 1: Similarities in ChessMaster and APT 10's attack chain

We first saw ChChes set its sights on an organization that's long been a target of APT 10/menuPass. As we caught and delved into more ChChes samples in the wild, however, we also saw how they followed the same pattern—exclusive packers, mutual targets, overlapping C&C infrastructure.

ChChes' packer, for instance, resembled the one used in menuPass' old PlugX samples. DNS records also showed that some of their command and control (C&C) servers and domains resolved to the same IP address, or resided in the same subnet. Are they operated by the same actors? Their commonalities make it appear so. It's also known to happen; BlackTech's cyberespionage campaigns are a case in point.

Figure 2: Comparison of Emdivi and ChChes

ChessMaster’s ChChes also resembles another backdoor, Emdivi, which first made waves in 2014. They have the same endgame. Both are second-stage payloads that use the system’s Security Identifier (SID) as encryption key so they execute only in their target’s machine. Their difference lies in complexity—ChChes hides part of the decryption key and payload in registry keys to make it harder to reverse engineer.

But that’s just one dot in several we’ve connected. In one instance, we detected PlugX and Emdivi on the same machine. This PlugX variant connected to an APT 10/menuPass-owned domain, but the packer is similar to that used by ChChes. While it’s possible it was hit by two different campaigns, further analysis told a different story. Both were compiled on the same date, only several hours apart. We detected and acquired the samples the next day, which means both backdoors were delivered to the victim a day after they were compiled.

Figure 3: Overview of the overlaps in ChessMaster and APT 10’s campaigns

Take ‘Control of the Center’

Ultimately attacks like ChessMaster’s make pawns out of the systems, networks, devices and their users, all of which hold the organization’s crown jewels. This is why enterprises need to be steps ahead of the game: prepare, respond, restore, and learn. Plan ahead—what techniques will attackers use? How can I defend against them? Don’t just pull the plug—understand what happened to better assess and mitigate the damage. Fine-tune your response—what worked, what didn’t, and what could’ve been done better?

Defense in depth plays a crucial role especially for the IT/system administrators and information security professionals that watch over them. The network, endpoints, servers, mobile devices, and web/email gateways are the bishops, knights, and rooks that underpin the enterprise’s crown jewels, which is why securing them is important. Reduce their attack surface. Keep the systems updated and regularly patched, and enforce the principle of least privilege. Employ behavior monitoring and application control. Deploy firewalls as well intrusion detection and prevention systems. Implement URL categorization, network segmentation, and data categorization.

ChessMaster’s gambit is spear-phishing, so it’s especially important to filter and safeguard the email gateway. Additionally, foster a cybersecurity-aware workforce. Seemingly benign icons or decoy documents can still swindle the victim, for instance. More importantly, develop proactive incident response and remediation strategies—threat intelligence helps enterprises prepare and mitigate attacks. Like in chess, the more you understand your enemy’s moves, the more successful you can be at thwarting them.

The Indicators of Compromise (IoCs) related to ChessMaster's campaigns is in this appendix.

This has been presented in the RSA Conference 2017 Asia Pacific & Japan as "ChessMaster: A New Campaign Targeting Japan Using the New ChChes Backdoor" on July 27, 2017, in Marina Bay Sands, Singapore. Updated on August 14, 2017, 11:50 PM to include IoCs related to ChessMaster.

Tags

Malware | Endpoints | Research