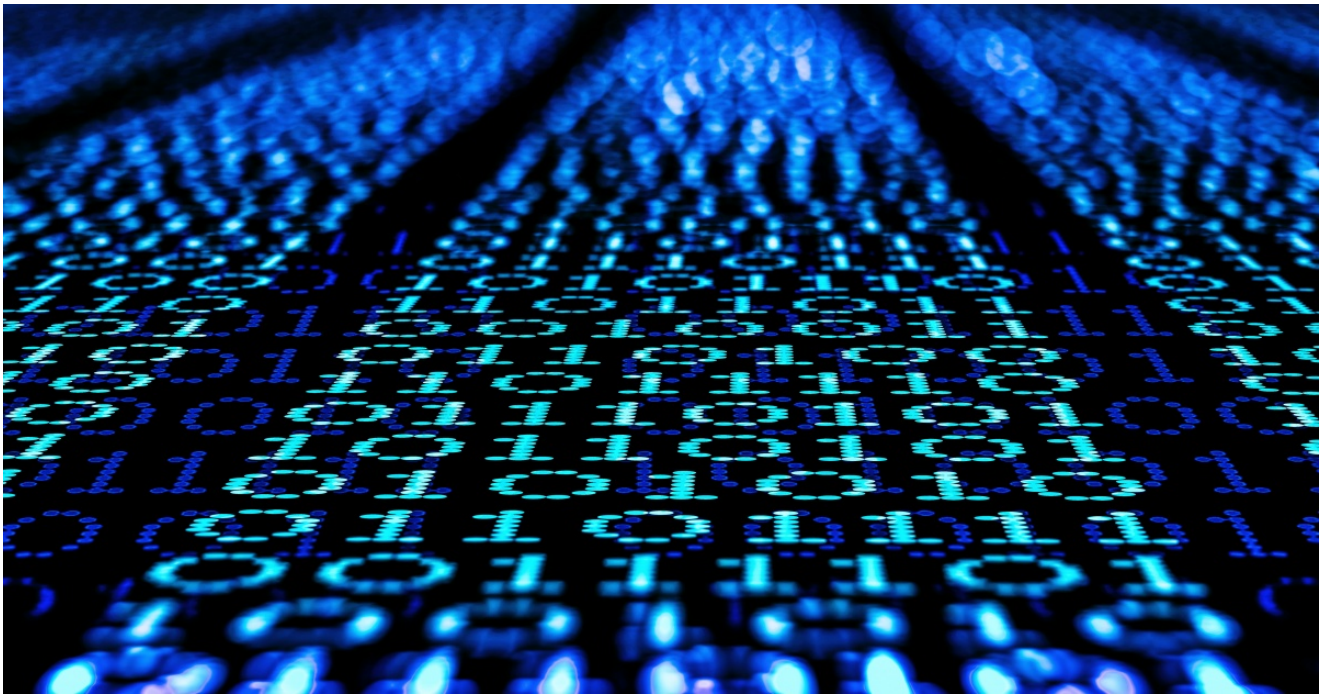
APT28: New Espionage Operations Target Military and Government Organizations

symantec.com/blogs/election-security/apt28-espionage-military-government



Threat Hunter TeamSymantec

Recent campaigns see APT28 group return to covert intelligence gathering operations in Europe and South America.

After making headlines during 2016 due to its involvement in cyber attacks against an organization involved in the U.S. presidential election, APT28 (aka Swallowtail, Fancy Bear) has continued to mount operations during 2017 and 2018.

The espionage group, which according to the U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) is linked to the Russian government, returned to low-key intelligence-gathering operations during 2017 and into 2018, targeting a range of military and government targets in Europe and South America.

History of disruptive attacks

APT28 has been active since at least January 2007 but received public attention in a major way during 2016 when it was implicated in a series of cyber attacks in the run up to the U.S. presidential election.

Beginning in the Spring of 2016, APT28 sent spear-phishing emails to political targets including members of the Democratic National Committee (DNC). These emails were designed to trick recipients into supposedly changing their email passwords on a fake webmail domain. The attack group then used these stolen credentials to gain access to the DNC network, install malware, move across the network, and steal data, including a trove of emails. The compromised information was later leaked online.

These election attacks signaled a change of tactics on the part of APT28, moving away from their prior low-key intelligence gathering towards more overt activity, seemingly intended to destabilize and disrupt victim organizations and countries.

The group was also responsible for the 2016 attack on the World Anti Doping Agency (WADA) and the leaking of confidential drug testing information. In keeping with its shift to more overt tactics, the group appeared to publicly take credit for the attack, leaking the information on a website using the name “Fancy Bears”, an industry codename that was already widely used for the group.

Return to the shadows

After receiving an unprecedented amount of attention in 2016, APT28 has continued to mount operations during 2017 and 2018. However, the group's activities since the beginning of 2017 have again become more covert and appear to be mainly motivated by intelligence gathering.

The organizations targeted by APT28 during 2017 and 2018 include:

- A well-known international organization
- Military targets in Europe
- Governments in Europe
- A government of a South American country
- An embassy belonging to an Eastern European country

Ongoing development of tools

APT28 uses a number of tools to compromise its targets. The group's primary malware is Sofacy, which has two main components. Trojan.Sofacy (also known as Seduploader) performs basic reconnaissance on an infected computer and can download further malware. Backdoor.SofacyX (also known as X-Agent) is a second stage piece of malware, capable of stealing information from the infected computer. A Mac version of the Trojan also exists (OSX.Sofacy).

APT28 has continued to develop its tools over the past two years. For example, Trojan.Shunnael (aka X-Tunnel), malware used to maintain access to infected networks using an encrypted tunnel, underwent a rewrite to .NET.

In addition to this, as reported by our peers at ESET last week, the group has also begun using a UEFI (Unified Extensible Firmware Interface) rootkit known as Lojax. Because the rootkit resides within a computer's flash memory, it allows the attackers to maintain a persistent presence on a compromised machine even if the hard drive is replaced or the operating system is reinstalled. Symantec products block attempts to install Lojax with the detection name Trojan.Lojax.

Possible links to other espionage operations

Another attack group, Earworm (aka Zebrocy), has been active since at least May 2016 and is involved in what appears to be intelligence gathering operations against military targets in Europe, Central Asia, and Eastern Asia. The group uses spear-phishing emails to compromise its targets and infect them with malware.

Earworm uses two malware tools. Trojan.Zekapab is a downloader component that is capable of carrying out basic reconnaissance functions and downloading additional malware to the infected computer. Backdoor.Zekapab is installed on selected infected computers and is capable of taking screenshots, executing files and commands, uploading and downloading files, performing registry and file system operations, and carrying out system information tasks. Earworm has also on occasion installed additional tools onto infected computers for the purposes of keylogging and password capture.

During 2016, Symantec observed some overlap between the command and control (C&C) infrastructure used by Earworm and the C&C infrastructure used by Grizzly Steppe (the U.S. government code name for APT28 and related actors), implying a potential connection between Earworm and APT28. However, Earworm also appears to conduct separate operations from APT28 and thus Symantec tracks them as a distinct group.

An ongoing threat

It is now clear that after being implicated in the U.S. presidential election attacks in late 2016, APT28 was undeterred by the resulting publicity and continues to mount further attacks using its existing tools. After its foray into overt and disruptive attacks in 2016, the group has

subsequently returned to its roots, mounting intelligence gathering operations against a range of targets. This ongoing activity and the fact that APT28 continues to refine its toolset means that the group will likely continue to pose a significant threat to nation state targets.

Protection

Symantec has had the following protections in place to protect customers against APT28 attacks:

- Trojan.Sofacy
- Backdoor.SofacyX
- Infostealer.Sofacy
- OSX.Sofacy
- Trojan.Shunnael
- Trojan.Lojax

The following protections are in place to protect customers against Earworm attacks:

- Trojan.Zekapab
- Backdoor.Zekapab

Threat Intelligence

Customers of the DeepSight Intelligence Managed Adversary and Threat Intelligence (MATI) service have received reports on the “Swallowtail” (also known as APT28), which detail methods of detecting and thwarting activities of this adversary.

File Attachments

APT28 indicators of compromiseTXT1.77 KB

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?