Cobalt Group Pushes Revamped ThreadKit Malware

Author:
Tom Spring
December 11, 2018
/ 1:40 pm

3 minute read

Skip to:
Reemergence of Cob

Share this article:

Threat actors have updated their malware to include a macro-based delivery framework.

Despite the high profile arrest earlier this year of the Cobalt Group ringleader, the threat actors behind the hacking collective are slowly ramping up their malicious behavior. In a new analysis of the threat group, known for its widespread attacks against banks in Eastern Europe over the past several years, the Cobalt Group has recently been observed updating its arsenal with a new version of the ThreadKit malware.

In a report issued by security firm Fidelis on Tuesday (PDF), researchers outline a number of new developments including:

- Despite an arrest earlier this year of a key member, of the Cobalt Group remains active.
- A new version on the malware ThreadKit is being actively distributed in October 2018.
- The CobInt trojan uses a XOR-based obfuscation technique.

Reemergence of Cobalt Group

The Cobalt Group first appeared in 2013 and in 2016 made a name for itself with widespread attacks on banks and ATM jackpotting campaigns across Europe. In one single campaign, it was credited for stealing over $32,000 from six Eastern Europe ATMs. In the following years the Cobalt Group expanded its focus to include financial-sector phishing schemes and new regions, including North and South America.

In March, the Cobalt Group was dealt a severe blow when the EUROPOL announced the arrest of the "criminal mastermind" behind the group in Alicante, Spain. Since then, the group was observed by Positive Technology in May as the criminals behind a spear phishing campaign directed at the financial sector that had the goal of enticing victims to download a JavaScript backdoor.

"In 2017 they expanded their targets from banks to include supply chain companies, financial exchanges, investment funds, and lenders in North America, Western Europe, and South America. Tools used in 2017 included PetrWrap, more_eggs, CobInt and ThreadKit," wrote Jason Reaves, principal, threat research with the Fidelis Threat Research Team in the report.

ThreadKit 2.0

After the arrest of Cobalt Group's leader, in May the group was spotted changing up its tactics. To that end, the Cobalt Group began focusing on exploits used for remote code execution found in Microsoft Word (CVE-2017-8570, CVE-2017-11882 and CVE-2018-0802) and one notably being the now patched April 2017 zero-day bug (CVE-2017-0199).

"In October 2018, [we] identified a new version of ThreadKit. As per Cobalt Group's typical methods, the malware was delivered via phishing email, containing a RFT Microsoft Office attachment which contained an evolved version of the exploit builder kit first uncovered in October 2017," according to Fidelis. "[This] new version of ThreadKit [utilizes] a macro delivery framework sold and used by numerous actors and groups."

Fidelis' latest analysis of the ThreadKit also notes "a slight evolution" in the exploit kit designed to better hide from detection. Obfuscation techniques include "placing the 'M' from the 'MZ' of an executable file into it's own object and now renaming a number of the objects inside."

Fidelis also pointed out the update including a new download URL where the malware code "objects" are downloaded from and later combined to create the executable. "A few highlights from the embedded files shows a check for block.txt, which is similar to the previous version's kill-switch implementation," Reaves wrote.

CobInt Adopts New Obfuscation Skills

The ThreadKit payload is the trojan CobInt, a longtime favorite of the Cobalt Group. To further frustrate analysis and detection, the attackers added another layer of obfuscation, a XOR routine used to decode the initial CobInt payload. A XOR, or XOR cipher, is an encryption algorithm that operates on a set of known principles. Encryption and decryption can be performed by applying and reapplying the XOR function.

"What's interesting here is that the XOR key is replaced by the subtraction value and the subtraction value is replaced by the previously read DWORD value. So the only value that's needed is the hardcoded XOR key, meaning mathematically this entire thing can be solved using a theorem prover such as Z3," researchers pointed out.

The decoded payload is the CobInt DLL, which when loaded will "sit in a loop beaconing to its C2 and waiting for commands and modules to be executed," according to Fidelis.

Fidelis and other researchers say the arrest of Cobalt group members have only temporarily slowed Carbanak/Cobalt threat actors. In a recent analysis by Kaspersky Lab, researchers said Cobalt arrests have only emboldened members and hastened the process of splitting the groups into smaller cells.

Share this article:

Cryptography Hacks Malware Vulnerabilities

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security
January 15, 2020 2

7 Tips for Maximizing Your SOC
December 31, 2019 5

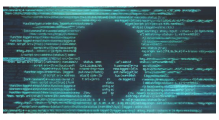
Mean Time to Hardening: The Next-Gen Security Metric
December 30, 2019 4

Combining AI and Playbooks to Predict Cyberattacks
December 26, 2019 1

The Case for Cyber-Risk Prospectuses
December 24, 2019 1

Twitter
#Magecart cybercriminals targeted the NutriBullet website for weeks, stealing the payment card data of its online c… https://t.co/cmaHwShKSZ
54 mins ago
Follow @threatpost

SUGGESTED ARTICLES



Innovative PureLocker Ransomware Emerges in Targeted Attacks
PureLocker is an example of the sustained and continuing efforts ransomware threat actors are putting into malware development.
November 14, 2019

FIN6 Switches Up PoS Tactics to Target E-Commerce
The group is using the More_eggs JScript backdoor to anchor its attack.
August 29, 2019

Oil and Gas Firms Targeted By New LYCEUM Threat Group
A new threat group has been discovered targeting Middle Eastern critical infrastructure firms with spearphishing emails laced with malware.
August 27, 2019

DISCUSSION