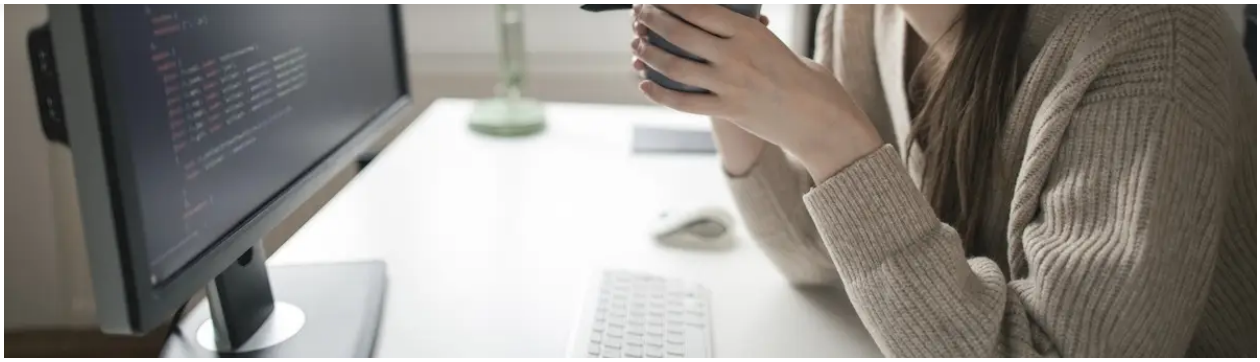
ITG08 (aka FIN6) Partners With TrickBot Gang, Uses Anchor Framework



Light Dark

April 7, 2020

By Ole Villadsen

6 min read

Advanced Threats

The past two years have borne witness to the increasing collaboration between organized cybercrime groups to avoid duplication of efforts and maximize profits. Although this collaboration has primarily occurred Threat Intelligence 's developing and distributing well-known banking Trojans, such as Emotet, TrickBot and IcedID, it does not stop there. In a new and dangerous twist to this trend, IBM X-Force Incident Response and Intelligence Services (IRIS) research believes that the elite cybercriminal threat actor ITG08, also known as FIN6, has partnered with the malware gang behind one of the most active Trojans — TrickBot — to use TrickBot's new malware framework dubbed "Anchor" against organizations for financial profit.

The Anchor malware framework itself is not new and its origins date back to at least 2018. It appears to be tightly connected to TrickBot and is likely programmed by the same malware authors that work on TrickBot. Cybersecurity firms SentinelOne and Cybereason have published reports in recent months describing Anchor as new malware developed by the TrickBot gang for use in targeted attacks against enterprises, including a new PowerShell-based backdoor called PowerTrick.

ITG08 and TrickBot — A Loaded Duo

ITG08/FIN6 is an organized cybercrime gang that has been active since 2015, primarily targeting point-of-sale (POS) machines in brick-and-mortar retailers and companies in the hospitality sector across the U.S. and Europe. TrickBot is a banking Trojan that emerged in 2016 and has since grown to be one of the top, and most sophisticated, Trojans being used by organized cybercrime gangs believed to be hailing out of Russia.

In the past six months, the Anchor backdoor malware, which includes a variant that communicates over DNS (Anchor_DNS), has been used in targeted attacks on enterprise networks — including POS systems — following initial infection by the TrickBot Trojan. The way organizations are being attacked ties with typical ITG08 activity reported throughout the past few years.

Through connecting our own findings with information from other security research reports, X-Force IRIS has determined that the threat actor ITG08 has partnered with the TrickBot gang to use that group's PowerTrick and Anchor backdoor malware for attacks on high-profile targets. This post provides more detail on that connection.

Tying ITG08 (FIN6) With Use of TrickBot's Anchor Framework

A past analysis by X-Force IRIS gave extensive information about ITG08's use of a backdoor known as "More_eggs". The gang's relationship with the boutique underground provider selling the TerraLoader loader and More_eggs backdoor leads to direct evidence of its use of PowerTrick and Anchor.

Bringing this cybercrime seller back into the picture, SentinelOne researchers reported observing a threat actor using PowerTrick and Anchor to download two samples developed and sold by the same seller: a TerraLoader that installs the More_eggs backdoor and a TerraLoader that deploys a signed Metasploit shellcode loader. The evidence provided below links these two samples to ITG08.

More_eggs Sample Analysis

X-Force IRIS is almost certain the TerraLoader and More_eggs samples were purchased by ITG08 based on similarities with two other More_eggs samples. We encountered the first sample in 2019 during an investigation of attacks we attributed to ITG08. We found the second sample, a Terraloader dropping a More_eggs backdoor, in a public repository that also showed ties to the ITG08 group.

Click and scroll to view
full table

Table 1: Comparison of three More_eggs samples and their command-and-control (C&C) domains

- All three C&C domains were created at the same time using the same email registration address.
- Two of the samples — the one downloaded by Anchor and the one attributed to ITG08 — use the same RKey, which is used in part to encrypt communications with the C&C host.
- Two of the TerraLoaders were compiled within two weeks of each other. The remaining TerraLoader could not be recovered.
- The RKey in the final sample, “wearenotcobaltthanks,” is a reference to the Cobalt Gang group, which previously had used the More_eggs backdoor. X-Force IRIS has found a similar message in other More_eggs samples attributed to ITG08: a variable called “Researchers” with the content, “We are not cobalt gang, stop associating us with such skids!”

Metasploit Shellcode Loader Sample Analysis

SentinelOne previously observed Anchor downloading a signed TerraLoader. That first step was followed by installing an Apache Bench executable hollowed out with a Metasploit loader shellcode that

received an RC4 encrypted payload.

X-Force IRIS lacks the sample hash or code-signing certificate to attribute this malware definitively to ITG08, but it is very similar to other samples we did attribute to the ITG08 group.

In 2019, X-Force IRIS observed ITG08 employ a signed Metasploit shellcode loader masquerading as the Apache Bench application and containing a Comodo code-signing certificate issued to "MAHTEM LTD." The shellcode was loaded into memory and designed to receive an RC4-encrypted buffer. This sample was used during an intrusion that featured the use of More_eggs.

X-Force IRIS identified a signed TerraLoader in a public repository that also decrypts a shellcode loader masquerading as Apache Bench. The sample used a code-signing certificate issued to "D. Bacte Ltd.", which we found in other samples that we attributed to ITG08 in some of our previous investigations.

More Evidence of ITG08's (FIN6) Fingerprints on TrickBot Malware

Further clues connect ITG08 to TrickBot and its operators' other malware. Generally speaking, the tactics used to deploy More_eggs in victim environments, as well as other threat actor tactics, techniques and procedures (TTPs) used during these Anchor campaigns, are unusually consistent with those used by ITG08.

More_eggs & TerraLoader Deployment

According to SentinelOne, the threat actor used PowerShell to download and execute a TerraLoader that installed More_eggs. X-Force IRIS has observed ITG08 employ the same tactic whereby it used PowerShell and Windows Management Instrumentation (WMI) to download and execute TerraLoader, then install More_eggs on remote hosts. X-Force IRIS has not observed any other actors who use More_eggs employ this tactic. Those who do typically install More_eggs only during the initial infection, after which they download additional malware or tools to proceed with

their intrusion phase.

TTPs Consistent With ITG08

In a blog about the subject, researchers from Cybereason noted that many of the threat actor TTPs they observed while using the Anchor framework were consistent with FIN6 activity, including the targeting of POS systems and the use of tools such as Metasploit, Cobalt Strike and AdFind.

X-Force IRIS has also encountered these TTPs in attacks that we attributed to ITG08. While these TTPs alone are insufficient to attribute the activity to ITG08, they are nevertheless fully consistent with ITG08 activity.

On a final note, X-Force IRIS is unaware of other threat actors deploying the combination of TerraLoader, More_eggs and Metasploit shellcode loaders in the manner described above. This activity, combined with the additional TTPs attributed to ITG08, such as the use of Metasploit, Cobalt Strike and AdFind while targeting POS systems, leads us to conclude with confidence that ITG08 is one of the threat actors using TrickBot's PowerTrick and the Anchor malware framework.

ITG08 Connecting to Evolve

ITG08's partnership with the TrickBot gang to use its Anchor malware framework is the latest example of a cybercriminal group that has repeatedly demonstrated its ability to adopt new malware and adapt to changing circumstances that threaten the group's ability to obtain illicit proceeds. In this respect, ITG08 behaves much like a commercial enterprise: adopting new technology, building strategic partnerships and grappling with changing markets by moving into new "lines of business" while leveraging their core strengths and outsourcing those of other groups.

ITG08's partnership with the TrickBot gang not only provides the group with new malware and potential access to enterprises infected with the TrickBot Trojan; it also reveals additional evidence of the group's strategy

to partner with other threat actors and malware developers. These varied relationships with elite cybercriminal actors and those who sell them tools, access and software allow ITG08 to continue to rely on its strengths in post-exploitation tactics, such as lateral movement, privilege escalation and data exfiltration, and outsource other attack vectors as needed.

The partnership with TrickBot is not the only evolution for ITG08. In recent years, this group has evolved to employ additional means to obtain illicit proceeds, including the targeting of e-commerce environments by injecting malicious code into online checkout pages of compromised websites in a modus operandi known as “Magecart.”

ITG08 also maintains established relationships with underground malware suppliers, such as the one responsible for developing and selling the TerraLoader loader and More_eggs JScript backdoor. ITG08 continues to benefit from its relationship with the developer behind More_eggs, whose malware features very low antivirus detection rates and makes use of other methods to evade detection, such as bypassing application whitelisting.

ITG08 has also been targeting e-commerce environments with a technique known as online skimming or grouped under what’s known as Magecart activity. In fact, ITG08 is the same group as Magecart Group 6. This relatively new activity almost certainly is a response to the adoption of EMV chips and point-to-point encryption.

ITG08 may also be part of attacks that deploy ransomware, such as Ryuk, LockerGoga and MegaCortex, again in likely partnership with banking Trojan botnets, which could be a further attempt to move into new “markets” that do not rely on the need to monetize credit card data.

Financially motivated, adaptable, sophisticated and persistent, ITG08 is likely to remain one of the most potent cybercriminal groups in this new decade.

Listen to a podcast episode on the impact of the ITG08 threat group

Indicators of Compromise (IoCs)

More_eggs C&C:

hxxps://drive.staticcontent[.]kz/drive/info

hxxps://metric.onlinefonts[.]kz/metric/inf

hxxps://host.moresecurity[.]kz/host/info

Metasploit Shellcode Loaders:

d9a245f1fb502606c226c364aa1090f25916e68f5ff24ef75be87ad6a2e6dcc9

d39f8aa90d54fd010484d7bb54c18549c3f03b02385020a35589dbe49e979bab

TerraLoaders dropping More_eggs:

dcf714bfc35071af9fa04c4329c94e385472388f9715f2da7496b415f1a5aa03

49af65995e51d88bbe8b0d4be5a5df2692aa57800f1875a18ecbd3f483c8a094

Banking Trojan | Collaboration | Command-and-Control (C&C) | Cybercrime | Cybercriminals | E-commerce | Finanacial Malware | Malware Analysis | Organized Crime | Point-of-Sale (POS) Systems | POS Malware | Ransomware | TrickBot | Trojan | X-Force

---

Ole Villadsen
Cyber Threat Hunt Analyst, IBM Security

POPULAR

ARTIFICIAL INTELLIGENCE | June 7, 2024

Open source, open risks: The growing