Understanding the relationship between Emotet, Ryuk and TrickBot

intel471.com/blog/understanding-the-relationship-between-emotet-ryuk-and-trickbot

By the Intel 471 Malware Intelligence team. One of the more notable relationships in the world of cybercrime is that between Emotet, Ryuk and TrickBot. This loader-ransomware-banker trifecta has wreaked havoc in the business world over the past two years, causing millions of dollars in damages and ransoms paid. Our Malware Intelligence team receives a lot of great questions from our clients on this subject, so we thought it would be good to do a Q/A style blog covering some of the more general questions.

Most perspectives on Ryuk come from a threat-hunting or incident-response point of view. In contrast, Intel 471's perspective is based on detailed knowledge of the malware itself and how it's being used. Our Malware Intelligence offering provides our clients with near real-time visibility into malware activity at the controller level. This activity includes infrastructure updates, new module/plugin downloads, targets being added to injects or configs, and many other data points.

Q: Are TrickBot campaigns operated by a single group?

A: TrickBot likely is operated by a single group as a malware-as-a-service (MaaS) platform that caters to a relatively small number of top-tier cybercriminals. Available information leads us to believe that individual TrickBot campaigns can be attributed to these different customers using the Group Tag (Gtag) parameter, and each customer may bring their own tactics, techniques and procedures (TTPs) and engage in highly targeted attacks.

Q: If multiple actors or groups are leveraging TrickBot, how is it possible to track the respective campaigns?

A: One technique is to focus on the Gtag parameter and map it to associated delivery methods. The Gtag value is hardcoded into each TrickBot sample and is thought to be a campaign identifier. For example, a Gtag could be "**fred372**," where "**fred**" is the group ID and the numerical value is thought to be a specific campaign or wave that can be linked to a method of delivery.

Q: How many different Gtag values are out there and why are they significant?

A: It's difficult to say exactly how many unique Gtag values there are, but we can offer some observations based on about 18 months of technical tracking and 37,000 unique TrickBot samples. We've seen about 1,000 unique Gtag values, but if we focus on just the group ID , there are only 59 unique values. The majority of samples in our data set — more than 92% — can be attributed to just a handful of group IDs — jim, lib, ono, sat and tot.

Furthermore, we can link the individual group IDs to specific spreading methods as previously mentioned. For example, It's suspected that **jimXX**, **libXX** and **totXX** are primarily delivered by malspam. We know that every **morXX**-related sample we observed was delivered via Emotet. All samples attributed to **sinXX**, **tinXX** and **winXX** were delivered via Bokbot aka IcedID. Samples attributed to **wmdXX** seem to utilize several different loaders, such as Amadey, FastLoader and an unnamed loader. Lastly, **satXX**, **summ1** and **trg1** all utilized the Ostap JavaScript loader for delivery.

Aside from the tracking perspective, Gtags also are significant from an incident response point of view. For example, if TrickBot samples are found in workstations and analysis shows them to be from **morXX** campaigns, getting rid of the TrickBot infection will not ensure the cleaning of the network, as there likely also will be Emotet binaries there.

Q: Are the Ryuk outbreaks connected with any specific Gtag?

A: Given the targeted and manual nature of Ryuk delivery, it's difficult to gain sufficient visibility into the samples to link them to specific Trickbot Gtags and Ryuk ransomware. However, from privately shared information, it appears that some Gtags are linked to the post-exploitation and deployment of Ryuk ransomware. The Gtag most often associated with Ryuk is said to be **morXX**. However, while the "mor" Group ID only surfaced in September 2019, the Trickbot to Ryuk connection has been observed since at least January 2019, and reportedly has been seen via other Gtags since then. One of those Gtags is **onoXX** which reportedly was linked to Ryuk attacks by several organizations in public information reports.

Q: Is there other specific behavior spotted with the morXX Gtag which has not been observed for other Gtag values?

A: Emotet malware typically is used as a loader for TrickBot campaigns, however, our monitoring registered 3 controller events — Feb. 7, 2020, April 1, 2020 and April 11 — where the roles were reversed and TrickBot Gtag **morXX** was used to download Emotet. Since August 2018 and across millions of controller events, we've not observed this behavior outside of these two examples. It suggests the actors behind **morXX** may have direct access to or some relationship with Emotet, however, the level and extent is unknown.

Q: It seems that in most of the Ryuk outbreaks, Emotet and TrickBot also were in the network. How does the chain work?

A: While it is true that many of the Ryuk incidents we've been privy to have involved both Emotet and TrickBot, it's important to specify where in the chain Ryuk enters. Emotet often is the precursor to TrickBot being loaded onto the system. TrickBot then uses several modules to carry out various activities on the victim system, allow for lateral movement and allow utilities such as BloodHound, Cobalt Strike and/or Empire to be loaded manually by the operators. The deployment of Cobalt Strike does not appear to be automated, but instead

is initiated on specific bots that match a profile. Once post-exploitation tools are loaded, the domain controller (DC) is attacked. When privileged access to the DC is acquired, Ryuk can be deployed across the network at the botnet operator's will.

Q: What is the best way to protect from Ryuk?

A: The first order of business for any organization is to have good security hygiene, including but not limited to ongoing security monitoring, a detection strategy, and response and recovery. There are at least two opportunities to stop both Emotet and TrickBot before a Ryuk outbreak occurs. The first is to stop Emotet from downloading TrickBot. The second is to stop TrickBot from spreading across the network, or at least stop it from communicating back to its command and control servers.

Once TrickBot has identified a domain controller on the network, the network defender is racing against the clock. If the infected machine is on a small-to-medium-sized business network, there is a very good chance threat actors will attack the domain controller and deploy Ryuk. Unfortunately, defensive measures such as anti-virus agents are unlikely to stop Ryuk, since the attacker can easily disable them (i.e., via a group policy object (GPO)).

Q: So, based on the capabilities of TrickBot mentioned above, is it still accurate to call it a banking trojan?

While TrickBot essentially is a banking trojan, the ability to extend its features by adding additional modules distinctly enhanced opportunities for groups running malware operations. Over the years we've seen TrickBot evolve from being a banker to an "all of the above" malware using case-specific modules.

Before the widespread use of ransomware, the actors behind Trickbot were engaged in fraudulent money transfer operations. The objective was to mass-infect as many computers as possible and look for high-value targets — individuals with high-balance bank accounts or small businesses. Using the banking trojan and web-injects, the botnet operators could make money transfers to money-mule accounts and then proceed to cash out. There are two problems with this operation:

1. Banks are getting better at detecting fraudulent transactions and eliminating money mule accounts.
2. These operations are high maintenance and very costly to operate because of the need to manage money mules, update web-injects, and maintain both the botnet infrastructure and the constant supply of new bots from new campaigns. While many of these things can be outsourced, each "partner" comes with added cost and risk.

With ransomware, the goals of the adversary remain the same, but the path to clean, laundered money is much shorter. Instead of dealing with money mules and bypassing access restrictions on banking accounts, the adversary convinces the victim to pay them directly in

bitcoins. Attackers no longer need to understand the intricacies of financial systems, since there now is a single blueprint that fits many targets: Find the domain controller and you have the keys to a network.

Q. What is the outlook for ransomware?

We've seen a number of things transpire in the world of cybercrime over the past three years as ransomware has taken the top spot for most lucrative malicious endeavors.

> The 2016 U.S. presidential election showed the world the power of exposing sensitive data and there's no doubt ransomware operators and developers were watching. It's now commonplace to see ransomware groups use blackmail tactics to compel victims to pay the ransom, while maintaining blogs to expose non-paying victims. In late 2019, the Maze ransomware team was the first to release data from non-paying ransomware victims, but the tactic subsequently was replicated by several ransomware-as-a-service (RaaS) operators. Intel 471 observed this tactic implemented by others, such as DoppelPaymer, MegaCortex, Nemty and REvil aka Sodinokibi. We'll continue to see this trend, giving companies yet another thing to worry about as they navigate the ransomware threat both to them directly, and the risk it brings them via their third-party vendors and suppliers.
>
> Emotet, Ryuk and Trickbot are by no means the only tools that team up to deliver ransomware. We've also observed connections between some Dridex and DanaBot actors, likely for ransomware delivery. MaaS operations cannot be written off as merely "commodity" malware, since their client pool includes very skilled groups that can and will cause serious damage if allowed to do so.
>
> Ransomware has helped revamp and boost a submarket where criminals can crowdsource the identification of potential targets. The sale of compromised accesses is nothing new in the underground marketplace, however, over the past 18 months there's been an explosion of such sales by actors ranging in sophistication from inexperienced to highly knowledgeable. Ransoms over the past three years have skyrocketed and now are in the millions in some cases, making ransomware operations a very lucrative activity. Purchasing a simple remote desktop protocol (RDP) access for thousands of dollars will provide a return on investment (ROI) for both sides of the sale. As malware-based vectors are considered, so too must the accesses being obtained through simple account takeovers or other means.