A Nasty Trick: From Credential Theft Malware to Business Disruption

fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html

Threat Research

Kimberly Goody, Jeremy Kennelly, Jaideep Natu, Christopher Glyer

Jan 10, 2019

11 mins read

Ransomware

Threat Research

Malware

FireEye is tracking a set of financially-motivated activity referred to as TEMP.MixMaster that involves the interactive deployment of Ryuk ransomware following TrickBot malware infections. These operations have been active since at least December 2017, with a notable uptick in the latter half of 2018, and have proven to be highly successful at soliciting large ransom payments from victim organizations. In multiple incidents, rather than relying solely on built-in TrickBot capabilities, TEMP.MixMaster used EMPIRE and RDP connections to enable lateral movement within victim environments. Interactive deployment of ransomware, such as this, allows an attacker to perform valuable reconnaissance within the victim network and identify critical systems to maximize their disruption to business operations, ultimately increasing the likelihood an organization will pay the demanded ransom. These operations have reportedly netted about $3.7 million in current BTC value.

Notably, while there have been numerous reports attributing Ryuk malware to North Korea, FireEye has not found evidence of this during our investigations. This narrative appears to be driven by code similarities between Ryuk and Hermes, a ransomware that has been used by APT38. However, these code similarities are insufficient to conclude North Korea is behind Ryuk attacks, as the Hermes ransomware kit was also advertised for sale in the underground community at one time.

It is important to note that TEMP.MixMaster is solely a reference to incidents where we have seen Ryuk deployed following TrickBot infections and that not all TrickBot infections will lead to the deployment of Ryuk ransomware. The TrickBot administrator group, which is suspected to be based in Eastern Europe, most likely provide the malware to a limited number of cyber criminal actors to use in operations. This is partially evident through its use of “gtags” that appear to be unique campaign identifiers used to identify specific TrickBot users. In recent incidents investigated by our Mandiant incident response teams, there has been consistency across the gtags appearing in the configuration files of TrickBot samples collected from different victim networks where Ryuk was also deployed. The uniformity of the gtags observed across these incidents appears to be due to instances of TrickBot being propagated via the malware’s worming module configured to use these gtag values.

Currently, we do not have definitive evidence that the entirety of TEMP.MixMaster activity, from TrickBot distribution and operation to Ryuk deployment, is being conducted by a common operator or group. It is also plausible that Ryuk malware is available to multiple eCrime actors who are also using TrickBot malware, or that at least one TrickBot user is selling access to environments they have compromised to a third party. The intrusion operations deploying Ryuk have also been called GRIM SPIDER.

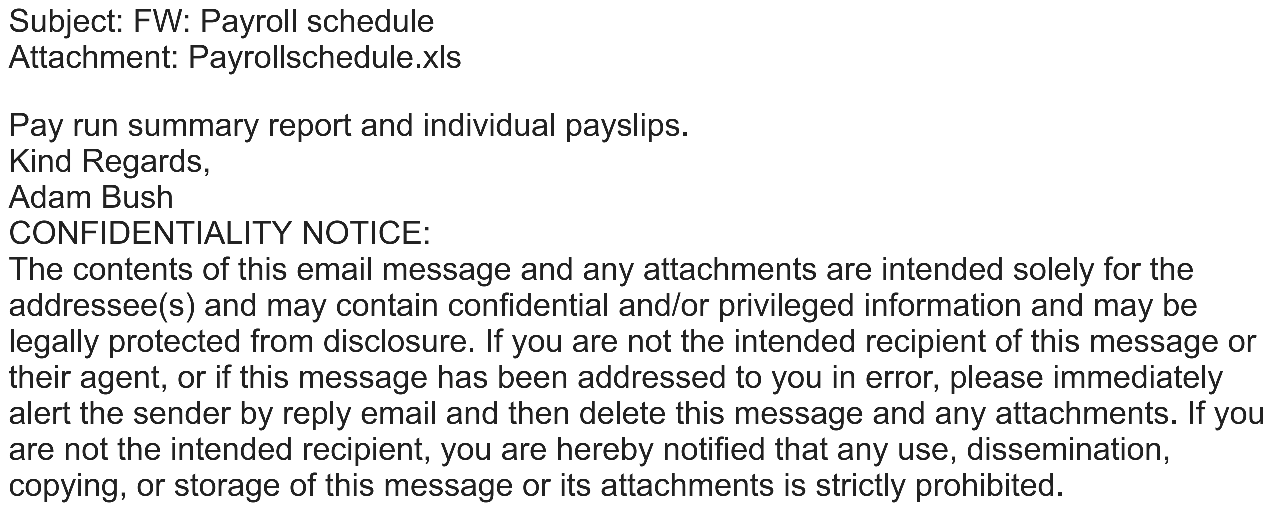
TrickBot Infection Leading to Ryuk Deployment

The following are a summary of tactics observed across incident response investigations where the use of TrickBot preceded distribution of Ryuk ransomware. Of note, due to the interactive nature of Ryuk deployment, the TTPs leading to its execution can vary across incidents. Furthermore, in at least one case, artifacts related to the execution of TrickBot were collected but there was insufficient evidence to clearly tie observed Ryuk activity to the use of TrickBot.

Initial Infection

The initial infection vector was not confirmed in all incidents; in one case, Mandiant identified that the attackers leveraged a payroll-themed phishing email with an XLS attachment to deliver TrickBot malware (Figure 1). Data from FireEye technologies shows that this campaign was widely distributed primarily to organizations in the United States, and across diverse industries including government, financial services, manufacturing, service providers, and high-tech.

Once a victim opened the attachment and enabled macros, it downloaded and executed an instance of the TrickBot malware from a remote server. Data obtained from FireEye technologies suggests that although different documents may have been distributed by this particular malicious spam run, the URLs from which the documents attempted to retrieve a secondary payload did not vary across attachments or recipients, despite the campaign's broad distribution both geographically and across industry verticals.



Subject: FW: Payroll schedule
Attachment: Payrollschedule.xls

Pay run summary report and individual payslips.
Kind Regards,
Adam Bush
CONFIDENTIALITY NOTICE:
The contents of this email message and any attachments are intended solely for the addressee(s) and may contain confidential and/or privileged information and may be legally protected from disclosure. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.

Figure 1: Email from a phishing campaign that downloaded TrickBot, which eventually led to Ryuk

Persistence and Lateral Movement

When executed, TrickBot created scheduled tasks on compromised systems to execute itself and ensure persistence following system reboot. These instances of TrickBot were configured to use their network propagation modules (sharedll and tabdll) that rely on SMB and harvested credentials to propagate to additional systems in the network. The number of systems to which TrickBot was propagated varied across intrusions from fewer than ten to many hundreds.

Dwell Time and Post-Exploitation Activity

After a foothold was established by the actors controlling TrickBot, a period of inactivity sometimes followed. Dwell time between TrickBot installation and Ryuk distribution varied across intrusions, but in at least one case may have been as long as a full year. Despite this long dwell time, the earliest reports of Ryuk malware only date back to August 2018. It is likely that actors controlling Trickbot instances used to maintain access to victim environments prior to the known availability of Ryuk were monetizing this access in different ways. Further, due to the suspected human-driven component to these intrusion operations, we would expect to commonly see a delay between initial infection and Ryuk deployment or other post-exploitation activity, particularly in cases where the same initial infection vector was used to compromise multiple organizations simultaneously.

Once activity restarted, the actors moved to interactive intrusion by deploying Empire and/or leveraging RDP connections tunneled through reverse-shells instead of relying on the built-in capabilities of TrickBot to interact with the victim network. In multiple intrusions TrickBot's reverse-shell module (NewBCtestDll) was used to execute obfuscated PowerShell scripts which ultimately downloaded and launched an Empire backdoor.

Variations in Ryuk Deployment Across Engagements

Post exploitation activity associated with each Ryuk incident has varied in historical and ongoing Mandiant incident response engagements. Given that collected evidence suggests Ryuk deployment is managed via human-interactive post-exploitation, variation and evolution in methodology, tools, and approach over time and across intrusions is expected.

The following high-level steps appear common across most incidents into which we have insight:

- Actors produce a list of targets systems and save it to one or multiple .txt files.
- Actors move a copy of PsExec, an instance of Ryuk, and one or more batch scripts to one or more domain controllers or other high privilege systems within the victim environment.
- Actors run batch scripts to copy a Ryuk sample to each host contained in .txt files and ultimately execute them.

Some of the notable ways Ryuk deployment has varied include:

- In one case, there was evidence suggesting that actors enumerated hosts on the victim network to identify targets for encryption with Ryuk, but in multiple other cases these lists were manually copied to the server that was then used for Ryuk distribution without clear evidence available for how they were produced.
- There have been multiple cases where TrickBot was deployed broadly across victim environments rather than being used to maintain a foothold on a small number of hosts.

- We have not identified evidence that Empire was used by the attackers in all cases and sometimes Empire was used to access the victim environment only after Ryuk encryption had started.
- In one case, the attackers used a variant of Ryuk with slightly different capabilities accompanied by a standalone .bat script containing most of the same taskkill, net, and sc commands normally used by Ryuk to terminate processes and stop services related to anti-virus, backup, and database software.

Example of Ryuk Deployment – Q3 2018

- Using previously stolen credentials the attacker logged into a domain controller and copied tools into the %TEMP% directory. Copied tools included AdFind.exe (Active Directory enumeration utility), a batch script (Figure 2), and a copy of the 7-Zip archive utility.
- Downloaded utilities were copied to C:\Windows\SysWOW64\.
- The attacker performed host and network reconnaissance using built-in Windows commands.
- AdFind.exe was executed using the previously noted batch script, which was crafted to pass the utility a series of commands that were used to collect information about Active Directory users, systems, OUs, subnets, groups, and trust objects. The output from each command was saved to an individual text file alongside the AdFind.exe utility (Figure 2).
- This process was performed twice on the same domain controller, 10 hours apart. Between executions of Adfind the attacker tested access to multiple domain controllers in the victim environment, including the one later used to deploy Ryuk.
- The attacker logged into a domain controller and copied instances of PSExec.exe, a batch script used to kill processes and stop services, and an instance of Ryuk onto the system.
- Using PsExec the attacker copied the process/service killing batch script to the %TEMP% folder on hundreds of computers across the victim environment, from which it was then executed.
- The attacker then used PsExec to copy the Ryuk binary to the %SystemRoot% directories of these same computers. A new service configured to launch the Ryuk binary was then created and started.
- Ryuk execution proceeded as normal, encrypting files on impacted systems.

```
adfind.exe -f (objectcategory=person) >  <user_list>.txt

adfind.exe -f objectcategory=computer > <computer_list>.txt

adfind.exe -f (objectcategory=organizationalUnit) > <ou_list>.txt

adfind.exe -subnets -f (objectCategory=subnet) > <subnet_list>.txt

adfind.exe -f "(objectcategory=group)" > <group_list>.txt

adfind.exe -gcb -sc trustdmp >  <trustdmp>.txt
```

Figure 2: Batch script that uses adfind.exe tool to enumerate Active Directory objects

Example of Ryuk Deployment – Q4 2018

- An instance of the EMPIRE backdoor launched on a system that had been infected by TrickBot. The attacker used EMPIRE's built-in capabilities to perform network reconnaissance.
- Attackers connected to a domain controller in the victim network via RDP and copied several files into the host's C$ share. The copied files included an instance of PsExec, two batch scripts, an instance of the Ryuk malware, and multiple .txt files containing lists of hosts within the victim environment. Many of the targeted hosts were critical systems across the victim environment including domain controllers and other hosts providing key management and authentication services.
- The attackers then executed the first of these two batch scripts. The executed script used PsExec and hard-coded credentials previously stolen by the actors to copy the Ryuk binary to each host passed as input from the noted .txt files (Figure 3).
- Attackers then executed the second batch script which iterated through the same host lists and used PsExec to execute the Ryuk binaries copied by the first batch script (Figure 4).

```
start PsExec.exe @C:\<shared_folder>$\<list>.txt -u <domain>\<username> -p
<password> cmd /c COPY "\\<shared_folder>\<ryuk_exe>" "C:\windows\temp\"
```

Figure 3: Line from the batch file used to copy Ryuk executable to each system

```
start PsExec.exe -d @C:\<shared_folder>$\<list>.txt -u <domain>\<username> -p
<password> cmd /c "C:\windows\temp\<ryuk_exe>"
```

Figure 4: Line from the batch file used to execute Ryuk on each system

Consistency in TrickBot Group Tags

Each individual TrickBot sample beacons to its Command & Control (C2) infrastructure with a statically defined “gtag” that is believed to act as an identifier for distinct TrickBot customers. There has been significant uniformity in the gtags associated with TrickBot samples collected from the networks of victim organizations.

- The instance of TrickBot identified as the likely initial infection vector for one intrusion was configured to use the gtag ‘ser0918us’.
    - At the time of distribution, the C2 servers responding to TrickBot samples using the gtag ‘ser0918us’ were sending commands to request that the malware scan victim networks, and then propagate across hosts via the TrickBot worming module.
    - It is possible that in some or all cases instances of TrickBot propagated via the malware’s worming module are configured to use different gtag values, specific to the same TrickBot client, designed to simplify management of implants post-exploitation.
- A significant proportion of TrickBot samples obtained from the victim environments, including in the case where the infection vector was identified as a sample using gtag ‘ser0918us’, had gtags in the below formats. This may suggest that these gtags are used to manage post-exploitation instances of TrickBot for campaigns distributed via gtag ‘ser0918us’ and other related gtags.
    - libxxx (ex: lib373, lib369, etc)
    - totxxx (ex: tot373, tot369, etc)
    - jimxxx (ex jim373, jim369, etc)
- The numbers appended to the end of each gtag appear to increment over time, and in some cases multiple samples sharing the same compile time but using different gtags were observed in the same victim environment, though in each of these cases the numbers appended to the end of the gtag matched (e.g. two distinct samples sharing the compile time 2018-12-07 11:28:23 were configured to use the gtags ‘jim371’ and ‘tot371’).
- The C2 infrastructure hard-coded into these samples overlaps significantly across samples sharing similar gtag values. However, there is also C2 infrastructure overlap between these samples and ones with dissimilar gtag values. These patterns may suggest the use of proxy infrastructure shared across multiple clients of the TrickBot administrator group.

Implications

Throughout 2018, FireEye observed an increasing number of cases where ransomware was deployed after the attackers gained access to the victim organization through other methods, allowing them to traverse the network to identify critical systems and inflict maximum damage. SamSam operations, which date back to late 2015, were arguably the first to popularize this methodology and TEMP.MixMaster’s is an example of its growing popularity with threat actors. FireEye Intelligence expects that these operations will continue to gain traction throughout 2019 due the success these intrusion operators have had in extorting large sums from victim organizations.

It is also worth highlighting TEMP.MixMaster’s reliance on TrickBot malware, which is more widely distributed, to gain access to victim organizations. Following indiscriminate campaigns, threat actors can profile victims to identify systems and users of interest and subsequently determine potential monetization strategies to maximize their revenue. Various malware families have incorporated capabilities that can aid in the discovery of high-value targets underscoring the necessity for organizations to prioritize proper remediation of all threats, not only those that initially appear to be targeted.

Acknowledgements

The authors would like to thank Brice Daniels, Edward Li, Eric Montellese, Sandor Nemes, Eric Scales, Brandan Schondorfer, Martin Tremblay, Isif Ibrahima, Phillip Kealy and Steve Rasch for their contributions to this blog post.