By FortiGuard SE Team | June 19, 2018

In conjunction with the Cyber Threat Alliance, Symantec today released their blog post on an APT (advanced persistent threat) group codenamed "Thrip." As part of our membership with the Cyber Threat Alliance (CTA), we have received these indicators ahead of publication to ensure that FortiGuard customers are protected from this latest disclosure.

Evidence suggests that the Thrip campaigns' objective was cyberespionage, with a focus on South East Asia and the United States. According to these latest findings, three computers in China have been identified as being used as a launchpad for these attacks. Targeted industries include defense, telecom, and satellite sectors, specifically the geospatial sector, where it targets computers running MapXtreme GIS (Geographic Information System) software. This software is used for tasks such as developing custom geospatial applications or integrating location-based data into various applications. It also targets machines running Google Earth Server and Garmin imaging software.

A potentially disruptive component to this threat was Thrips' targeting of a satellite communications operator, and once a foothold was established, utilizing lateral movement techniques to specifically locate and infect those devices that monitor and control satellites. Symantec noted that such an attack suggests that the attackers may have not only wanted to gather intelligence and exfiltrate data, but also potentially disable the satellites themselves.

Thrip Versatility

One of the most interesting aspects of the Thrip attack campaign is its ability to leverage a number of techniques and open source and publicly available tools to achieve its objectives.

- ***PsExec***: A Microsoft Sysinternals tool for executing processes on other systems, making it useful for remote administration. The tool is primarily used by the attackers to move laterally across a victim's network. Because it is widely used for legitimate purposes, its misuse can be difficult to detect, or if detected, to attribute to a malicious activity or a specific threat actor.
- ***PowerShell***: A Microsoft scripting tool that can be used by system administrators to issue administrator level commands, move laterally around a network, and download files. Because of this ability, attackers using PowerShell can potentially evade detection while maintaining a strong foothold on any compromised systems.
- ***Mimikatz***: Thrip also used this freely available tool that is capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext. This tool is legitimately used by pen testers, but attackers often use it as well because of its unique capabilities.
- ***WinSCP***: This open source FTP client is used by Thrip to exfiltrate data from targeted organizations.
- ***LogMeIn***: Cloud-based remote access software. It's still unclear whether the attackers are able to gain unauthorized access to a victim's LogMeIn accounts or whether they simply create their own.
- ***Infostealer***: Thrip was also observed remotely installing infostealer malware in order to exfiltrate credentials and system information. This updated version contains additional features designed to evade anti-virus technology, as well as the ability to capture information from new applications (such as web browsers) that have become available since the original info stealing malware sample was created.

Lateral Movement Techniques

Thrip exemplifies the growing urgency for being able to quickly and reliably detect lateral movement across the network, which is not easily done using legacy security systems. This sort of countermeasure requires keeping up with the latest techniques adversaries are using, while being proactive in finding and addressing existing network blind spots and control gaps.

Breaching a network requires finding a device that can be compromised in order to enable a sophisticated attack to establish a beachhead. However, that initial machine rarely contains the information that attackers are looking for. To achieve their objective, they then need to be able to move laterally across the network looking for the right systems to complete their cyber mission, as well as to establish a stronger foothold to increase the difficulty of properly removing the malware from the network.

Detecting an initial compromise can be very difficult, even with sophisticated security measures in place, as it usually happens very fast and often uses advanced evasion techniques to disguise the attack. But once an adversary begins to move laterally across a network probing for its data target, its increased activity gives security analysts a better chance to identify it.

While there are a lot of tactics and techniques an adversary can use to move across a network, there are three key steps they all must take in order to move their malware from system to system.

1. Gaining the right access privileges

Attackers are aware that malware detection technologies are constantly evolving, making it a cybersecurity event a game of cat and mouse. Attackers know that in order to evade detection and any other technological defenses, attackers have to be careful in planning their method of attack. The Thrip campaign is an example of attackers using publicly available tools in combination with their own custom set of solutions. This allows them to "operate in the shadows," which means that the attacker is operating in the network and its various systems using tools that might not necessarily be considered malicious. Because these tools are regularly used by system administrators, red/blue teams, and pen testers, their use is often ignored. Because of this, discovering a compromise often occurs too late, and attributing an attack to a specific group or threat actor can be extremely difficult.

In order to move laterally across a network undetected, an attacker requires the right access privileges. Most attackers use a combination of open source and publicly available tools and custom malicious software to gain and escalate privilege. There are many ways to gain the right access privileges, such as stealing the following data:

- LM and NT hashes found in the LSASS process, as well as in local accounts in the SAM registry hive
- Delegate tokens used in single sign-on.
- Cached credentials found in the registry to enable login capabilities when not connected to the network.
- LSA Secret information which has password information in the registry for accounts that run services, VPN accounts, scheduled tasks, etc.
- Tickets which are used issued to an authenticated user when using the Kerberos protocol.

Various open source and proprietary tools can be used to steal any of these. Other access privilege attacks include creating a new account on a network and then escalating its privileges, or (less frequently anymore) using a brute force attack to obtain passwords. In the case of Thrip, the threat actors used a custom malicious Infostealer to gain access to its targets, along with a combination of post exploitation tools (mimikatz) to perform even more lateral movement in order to gain an even stronger network foothold.

2. Copying the malware to other systems

Once an attacker has acquired the right access privileges, they need to copy their malware from their original system to the targeted device. To do this, attackers often use some sort of remote desktop tool like RDP, VNC, or Team Viewer, which have all been used in real attacks. Thrip used Microsoft's PsExec Sysinternals remote administration tool to copy the malware to other devices. There are a number of other ways to achieve this. A recent attack from the Orangeworm group that targeted Healthcare networks simply used admin shares to copy their malware from system to system. Script-based techniques copy malware to admin shares such as C$, ADMIN$ and IPC$, which are usually available on many networks today.

3. Execute the malware on targeted system

Finally, an attacker needs to run the malware, which can happen in a few different ways:

- PsExec, which was used by Thrip, allows an attack to copy and remotely execute malware.
- PowerShell and WMI are other tools used by administrators that can also be used by attackers to remotely execute malware. (Invoke-WmiMethod, Invoke-Command, Enter-PSSession.)

- Remote Management Tools, such as SC, AT, WinRS ,and Schtasks, can add tasks that can be scheduled to run at certain times of the day.
- Malware can also spread using worm-like propagation techniques that can identify vulnerabilities left open by poor security hygiene. A recent example is the spreading of WannaCry using the infamous Eternal Blue exploit given to us by Shadow Brokers.

Other Thrip Attack Tools

A number of notable malware samples used by the Thrip actors were also observed:

- ***W32/Trojan.A!tr***: This is a custom Trojan designed to steal information from an infected computer, including credentials and system information.
- ***W32/Agent.DPFP!tr.bdr***: Based on ***W32/Trojan.A!tr***, this malware contains additional features designed to avoid detection. It also includes a number of new capabilities such as the ability to capture information from newer applications (such as new or updated web browsers) that have emerged since the original ***W32/Trojan.A!tr*** malware was created.
- ***W32/Agent.WAPO!tr***: This is a keylogger known to have been created by underground Chinese hackers. Although publicly available, it is not frequently seen.
- ***W32/BackDoor.A!tr***: Although not seen in this recent wave of attacks, this is a backdoor Trojan that has been used by Thrip in other campaigns.
- ***W32/Syndicasec.C!tr***: This is another Trojan that has been used by Thrip in previous campaigns.

Solution

The FortiGuard Labs team has seen attackers start to incorporate techniques to further their ability to avoid detection. Just like any project, developing these attacks takes considerable effort, resources, and possibly capital, and attackers are playing the long game. What this means is that attackers often have a carefully developed business plan where their return on investment pays off, to the detriment of the victims.

Defending against an advanced threat such as Thrip requires a number of critical security strategies to be in place. FortiGuard Labs recommends the following:

1. ***Maintain security hygiene***. Many advanced attacks start by compromising a vulnerable device. And for the vast majority of cyber events, those devices are compromised because they weren't properly patched, updated, or protected. Establishing security hygiene involves inventorying all devices on the network, identifying vulnerabilities, and rating related risks. *We also recommend a proactive and just in time patching schedule, along with ensuring that the latest up to date FortiGuard definitions are applied when they are available.*
2. ***Segment your network***. It is critical that today's networks are fully segmented, from the access layer to the data center. Establishing clear lines of defense and enforcing deep inspection at segment check points helps protect critical resources from the sort of lateral movement attacks most advanced threats require.
3. ***Baseline normal behavior***. Sophisticated threats like Thrip often hijack common—and authorized—administration tools in order to escalate privileges, spread malware, and execute an attack. These sorts of activities are difficult to detect without first understanding when one of these tools is behaving in an unexpected manner. Addressing this requires baselining normal behavior in the network, such as user activities, device traffic patterns, and administration and management tool usage. This allows any misuse of these resources to be automatically flagged and any related countermeasures to be triggered.

Integration and Automation are Key

The time to detect a security event is often measured in weeks or months, especially if security devices operate as siloed systems. In the case of an attack like Thrip, this lag between compromise and detection can result in a serious and even catastrophic failure of critical systems. That's because security teams have to scan and hand correlate event and log files between isolated devices looking for suspicious events. This becomes increasingly difficult as attacks adopt more sophisticated evasion techniques.

To counter this challenge, security tools need to be able to leverage common operating systems,

open standards, and single pane of glass management and analysis tools in order to dynamically share and correlate local threat intelligence with external threat feeds. Automation then needs to put in place to allow your cybersecurity solutions to operate as a single, integrated fabric.
This architectural-based approach enables security systems to dynamically coordinate a unified response to any detected threats at digital speeds anywhere across the entire distributed network.
Kind Regards,