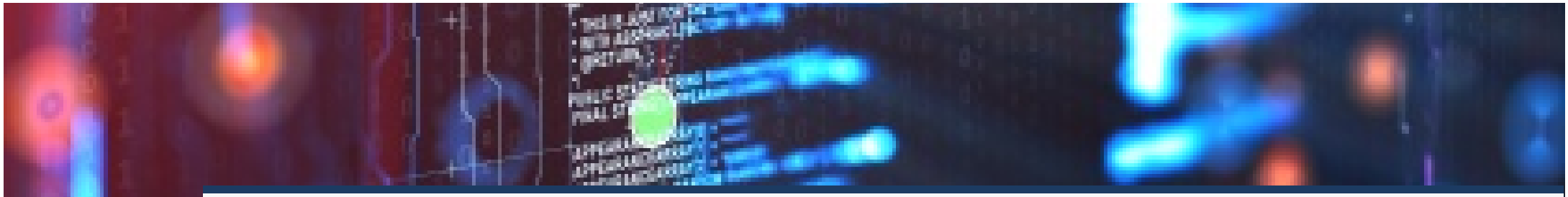


Security Response Attack Investigation Team

POSTED: | MIN READ | THREAT INTELLIGENCE

SUBSCRIBE FOLLOW

SHARE

One of the most significant developments in cyber espionage in recent years has been the number of groups adopting "living off the land" tactics. That's our shorthand for the use of operating system features or legitimate network administration tools to compromise victims' networks. The purpose of living off the land is twofold. By using such features and tools, attackers are hoping to blend in on the victim's network and hide their activity in a sea of legitimate processes. Secondly, even if malicious activity involving these tools is detected, it can make it harder to attribute attacks. If everyone is using similar tools, it's more difficult to distinguish one group from another. Most attack groups do still create and leverage custom malware, but it tends to be employed sparingly, reducing the risk of discovery.

Finding the needle in the haystack

This doesn't mean espionage attacks are now going undiscovered, but it does mean that they can take longer for analysts to investigate. This is one of the reasons why Symantec created Targeted Attack Analytics (TAA), which takes tools and capabilities that we've developed for our own analysts and makes them available to our Advanced Threat Protection (ATP) customers. TAA leverages advanced artificial intelligence and machine learning that combs through Symantec's data lake of telemetry in order to spot patterns associated with targeted attacks. Its advanced AI automates what previously would have taken thousands of hours of analyst time. This makes it far easier for us, and for our customers, to find that needle in the haystack.

It was TAA that led us to the latest cyber espionage campaign we've uncovered. Back in January 2018, TAA triggered an alert at a large telecoms operator in Southeast Asia. An attacker was using PsExec to move laterally between computers on the company's network. PsExec is a Microsoft Sysinternals tool for executing processes on other systems and is one of the most frequently seen legitimate pieces of software used by attackers attempting to live off the land. However, it's also widely used for legitimate purposes, meaning malicious use of PsExec can be difficult to spot.

TAA not only flagged this malicious use of PsExec, it also told us what the attackers were

using it for. They were attempting to remotely install a previously unknown piece of malware on computers within the victim's network. When we analyzed the malware, we discovered that it was an updated version of Trojan.Rikamanu, malware associated with Thrip, a group we've been monitoring since 2013. After further investigation, we discovered that Thrip also used a completely new piece of malware in this attack (Infostealer.Catchamas).

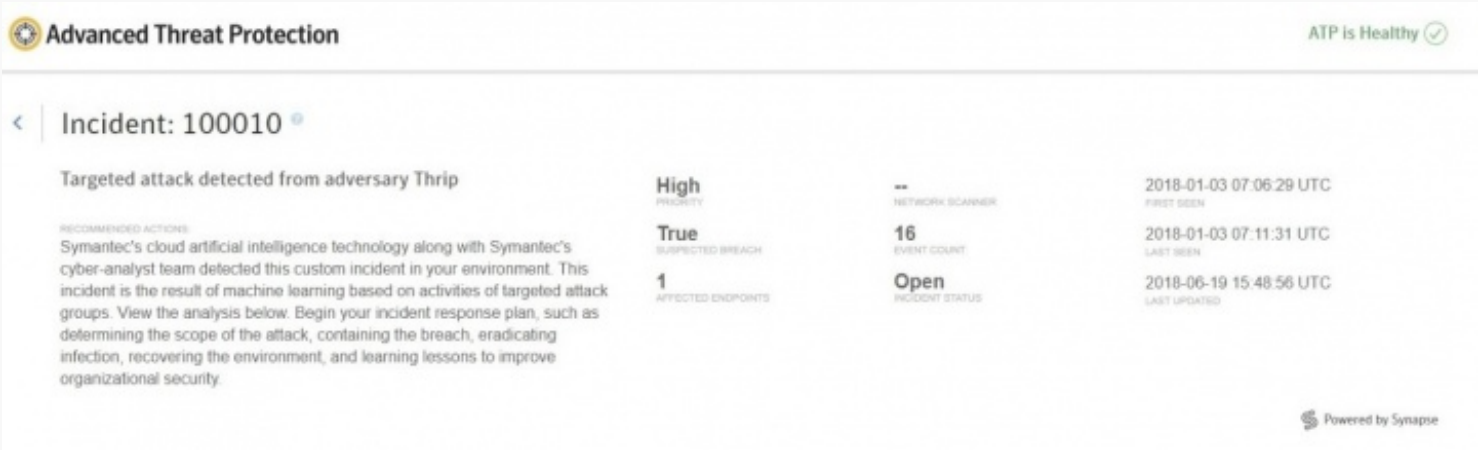


Figure 1. Targeted Attack Analytics leverages machine learning to spot malicious activity associated with targeted attacks and alerts the customer.

Armed with this information about the malware and living off the land tactics being used against this victim, we broadened our search to see if we could find similar patterns that indicated Thrip had been targeting other organizations. We uncovered a wide-ranging cyber espionage campaign involving powerful malware being used against targets that are a

cause for concern.

We identified three computers in China being used to launch the Thrip attacks. Thrip's motive is likely espionage and its targets include those in the communications, geospatial imaging, and defense sectors, both in the United States and Southeast Asia.

Eye on the sky: Thrip's targets

Perhaps the most worrying discovery we made was that Thrip had targeted a satellite communications operator. The attack group seemed to be particularly interested in the operational side of the company, looking for and infecting computers running software that monitors and controls satellites. This suggests to us that Thrip's motives go beyond spying and may also include disruption.

Another target was an organization involved in geospatial imaging and mapping. Again, Thrip seemed to be mainly interested in the operational side of the company. It targeted computers running MapXtreme GIS (Geographic Information System) software which is used for tasks such as developing custom geospatial applications or integrating location-based data into other applications. It also targeted machines running Google Earth Server and Garmin imaging software.

The satellite operator wasn't the only communications target Thrip was interested in. The

group had also targeted three different telecoms operators, all based in Southeast Asia. In all cases, based on the nature of the computers infected by Thrip, it appeared that the telecoms companies themselves and not their customers were the targets of these attacks.

In addition, there was a fourth target of interest, a defense contractor.

Figure 2. Thrip, spying on communications, mapping, and defense targets

Attempting to hide in plain sight

We've been monitoring Thrip since 2013 when we uncovered a spying campaign being orchestrated from systems based in China. Since our initial discovery, the group has changed its tactics and broadened the range of tools it used. Initially, it relied heavily on custom malware, but in this most recent wave of attacks, which began in 2017, the group has switched to a mixture of custom malware and living off the land tools. The latter include:

- **PsExec**: Microsoft Sysinternals tool for executing processes on other systems. The tool was primarily used by the attackers to move laterally on the victim's network.
- **PowerShell:** Microsoft scripting tool that was used to run commands to download payloads, traverse compromised networks, and carry out reconnaissance.
- **Mimikatz:** Freely available tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext.
- **WinSCP:** Open source FTP client used to exfiltrate data from targeted organizations.
- **LogMeIn:** Cloud-based remote access software. It's unclear whether the attackers gained unauthorized access to the victim's LogMeIn accounts or whether they created their own.

All of these tools, with the exception of Mimikatz (which is almost always used maliciously), have legitimate uses. For example, PowerShell is widely used within enterprises and the vast majority of scripts are legitimate. Similarly, PsExec is frequently used by systems administrators. However, in this case, it was Thrip's use of PsExec that drew our attention. Through advanced artificial intelligence and machine learning, TAA has trained itself to spot patterns of malicious activity. While PsExec itself may be innocuous, the way that it was being used here triggered an alert by TAA. In short, Thrip's attempts at camouflage blew its cover.

While Thrip now makes heavy use of living off the land tactics, it also employs custom

malware, particularly against computers of interest. This includes:

- **Trojan.Rikamanu**: A custom Trojan designed to steal information from an infected computer, including credentials and system information.
- **Infostealer.Catchamas**: Based on Rikamanu, 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 Trojan.Rikamanu malware was created.
- **Trojan.Mycicil:** A keylogger known to be created by underground Chinese hackers. Although publicly available, it is not frequently seen.
- **Backdoor.Spedear:** Although not seen in this recent wave of attacks, Spedear is a backdoor Trojan that has been used by Thrip in other campaigns.
- **Trojan.Syndicasec:** Another Trojan used by Thrip in previous campaigns.

Highly targeted espionage operation

From the initial alert triggered by TAA, we were able to follow a trail that eventually enabled us to see the bigger picture of a cyber espionage campaign originating from computers within China and targeting multiple organizations in the U.S. and Southeast Asia. Espionage is the group's likely motive but given its interest in compromising operational systems, it could also adopt a more aggressive, disruptive stance should it choose to do so.

Protection

Symantec has had protection from Thrip since 2013 and we secure our customers from the attack group's latest set of malicious tools. The following protections are in place to protect customers against Thrip attacks:

File-based protection

- Trojan.Rikamanu
- Infostealer.Catchamas
- Hacktool.Mimikatz
- Trojan.Mycicil
- Backdoor.Spedear
- Trojan.Syndicasec

Network Protection Products

- Malware Analysis Appliance detects activity associated with Thrip
- Customers with Webpulse-enabled products are protected against activity associated with Thrip

Threat Intelligence

In addition to file-based protection, customers of the DeepSight Intelligence Managed Adversary and Threat Intelligence (MATI) service have received multiple reports on Thrip (codenamed ATG14) which detail methods of detecting and thwarting activities of this group.

File Attachments

Thrip IOC list | TXT | 10.14 KB

Further reading

To find out more about Targeted Attack Analytics (TAA), read our whitepaper Targeted Attack Analytics: Using Cloud-based Artificial Intelligence for Enterprise-Focused Advanced Threat Protection

About the Author

Security Response Attack Investigation Team

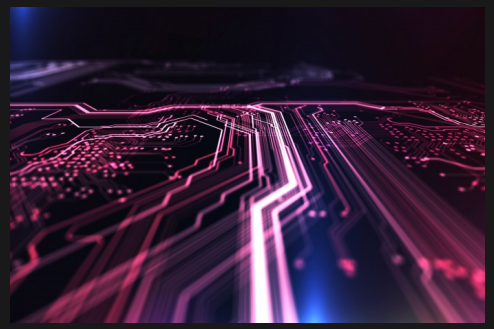
The Attack Investigation Team is a group of security experts within Symantec Security

Response whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis which helps customers respond to attacks.

Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

Related Blog Posts



POSTED: | MIN READ

POSTED: | MIN READ

POSTED: | MIN READ

POSTED: | MIN

READ