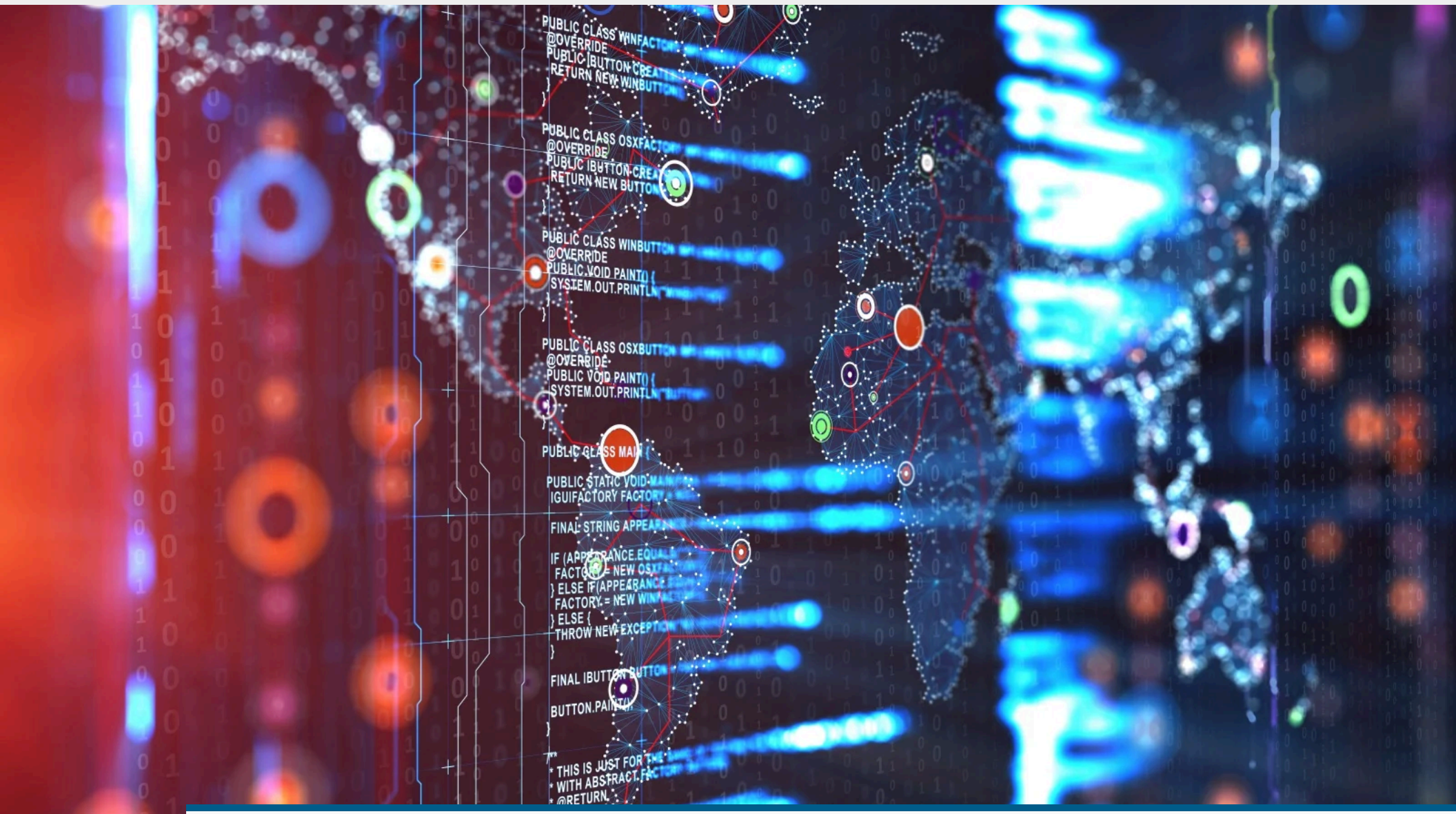


Threat Hunter Team
Symantec

POSTED: 19 JUN, 2018 | 5 MIN READ |
THREAT INTELLIGENCE

SUBSCRIBE FOLLOW

Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies

SHARE

Symantec's artificial-intelligence-based Targeted Attack Analytics uncovers new wide-ranging espionage operation.

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 u
compro
such fea
hide the
involvin
is using
attack g
employed sparingly, reducing the risk of discovery.

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our Cookie Policy.

Accept Cookies

Cookies Settings

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 (Infostealer.Catchamas) on computers within the victim's network.

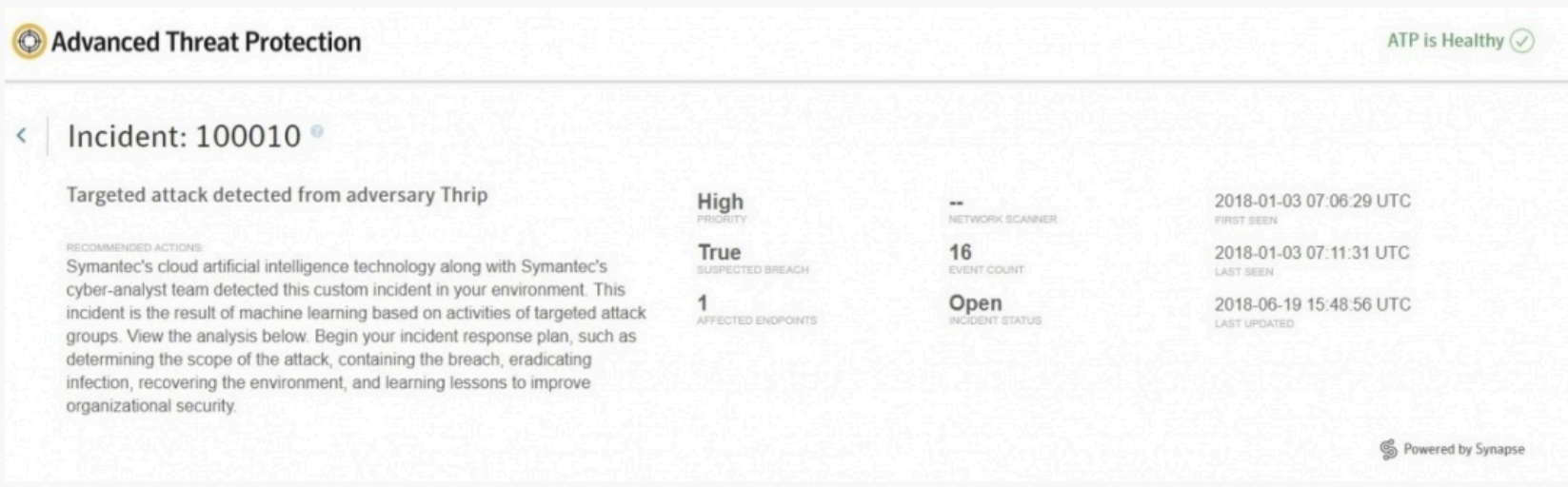


Figure 1. Targeted Attack Analytics leverages machine learning to spot malicious activity associated with targeted attacks and alerts the customer.

Armed with this inform
used by this group of a
see if we could find sin
organizations. We unc
powerful malware beir

We identified three co
Thrip's motive is likely

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

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 Geographic Information System (GIS) 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.

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

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

Attempting to hide in plain sight

Thrip uses a mixture of custom malware and living off the land tools to perform its attacks. The latter include:

- **PsExec**: Microsoft
  The tool was prima
  network.
- **PowerShell:** Micro
  payloads, traverse
- **Mimikatz:** Freely a
  certificates, and re

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

- **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 (Infostealer.Catchamas), particularly against computers of interest. Catchamas is a custom Trojan designed to steal information from an infected computer and contains additional features designed to avoid detection.

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

The following protections are in place to protect customers against Thrip attacks:

File-based protection

- Infostealer.Catchamas
- Hacktool.Mimikatz

Network protection p

- Malware Analysis A
- Customers with W
  associated with Th

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

Threat intelligence

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

File Attachments

Thrip IOC list | TXT | 564 bytes

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

Threat Hunter Team

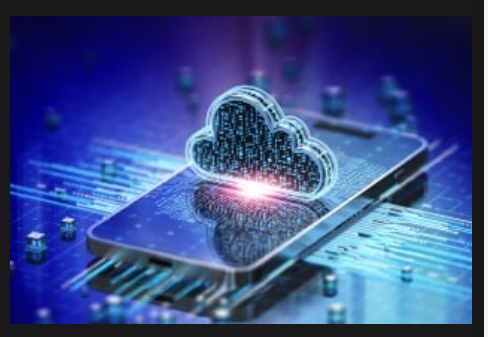
Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that 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: 22 OCT, 2024 | 5 MIN READ

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**

Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

Ransomware: Threat Level Remains High in Third Quarter

Stonefly: Extortion Attacks Continue Against U.S. Targets

Ransomware: Attacks Once More Nearing Peak Levels

SUBSCRIBE FOLLOW

Privacy Policy Cookie Policy Data Processing and Data Transfers Supplier Responsibility Terms of Use Sitemap

Copyright © 2005-2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Cookies

By clicking Accept Cookies, you understand that Broadcom and third-party partners use technology, including cookies to, among other things, analyze site usage, improve your experience and help us advertise. For more details, please see our **Cookie Policy.**