AUGUST 2021

Threat Hunter Intelligence Report

Emerging Threats

splunk>
turn data into doing™

The Threat Hunter Intelligence Report is a monthly series brought to you by Splunk's threat hunting and intelligence (THI) team. We research and produce actionable reports on the latest cybersecurity threats and trends — helping organizations stay one step ahead of adversaries, one report at a time.

Emerging threats 101

These days, cybercriminals are incredibly ambitious, working overtime to develop threats that devastate high-stakes targets. And if detected, they have no shortage of tools at their disposal. Some of the latest weapons in their arsenal include fileless malware attacks — malicious code that piggybacks on legitimate software and bypasses familiar detection mechanisms. Cybercriminals are also applying adaptive machine learning technologies to malware to better evade detection, and have upped their ransomware game by going deep into high-value business targets.

And it doesn't stop there. Attackers are taking advantage of vulnerabilities in supply chains, targeting the operational weaknesses of specific organizations and exploiting new attack surfaces opened up by cloud services. Unsurprisingly, cybercriminals are also tapping into the fear and uncertainty around COVID-19, with new threats surfacing like the COVID-19 vaccine phishing campaigns and brute force attacks against Microsoft's remote desktop protocol (RDP), both of which target a newly remote workforce.

To protect against increasingly cunning perpetrators, these types of emerging threats mean reimagining security defenses. Our latest issue examines evolving threat techniques, intended targets and what security teams can do to be better equipped for facing the unknown.

THI profile 1

Katana and Amnesia attacks target IoT

Believe it or not, there are now over 50 billion connected devices that are part of the Internet of Things (IoT). But this doesn't come without risks. More IoT devices inevitably means more gaps in cybersecurity, with serious threats to be faced across industries like shipping, manufacturing, engineering, transportation and energy. Bad actors are now exploiting the interconnectivity of IoT devices, particularly the lack of cybersecurity standards and regulations governing them.

Two recent major IoT attacks exposed massive security flaws. In late October 2020, researchers discovered a new IoT virus called Katana, which infected hundreds of IoT devices daily. Available on the darknet, this advanced virus uses remote code execution and command injection instructions to exploit IoT security vulnerabilities.

Another recent (and even more devastating) IoT threat is nicknamed Amnesia:33. This batch of vulnerabilities takes advantage of the millions of consumer and enterprise IoT devices that have as many as 33 coding flaws in their open source TCP/IP stacks, unintentionally allowing for remote code execution, denial of service or a complete takeover of a device.

What you need to know:

Companies that rely on IoT need to be aware of the data inputted into these devices and implement the appropriate security protections. Consider contacting the device manufacturers to ensure that you have maximized all possible security features on your devices. IoT is showing no signs of slowing down, and the market will continue to grow exponentially over the coming years, increasing the number and severity of new IoT-based cyberattacks.

THI profile 2

DanaBot brings malware back into style

Sometimes old tricks come back in style. DanaBot — one of the most widely distributed banking trojans from 2018 to 2020 — experienced a sharp decline until its resurrection in June 2020. Now it's back, and it poses a bigger threat than ever.

When DanaBot first came on the scene in 2018, hackers targeted Australian users via phishing campaigns before going on to develop a second variant targeting U.S. companies. Eventually, a third variant was discovered by ESET researchers in February 2019, wreaking havoc with its remote command-and-control function. Compared to previous campaigns, the variant that reemerged in late 2020 is packed with a deadly arsenal of tools, including a ToR component to anonymize communications between the attackers and the point of infection.

And it gets better: DanaBot distributes malware under the guise of software keys and cracks — including anti-virus software, graphics editors, computer games and more. Once the unsuspecting victim downloads these files, they unleash a bundle of malware types into their system — including the ever-insidious DanaBot.

What you need to know:

These software cracks are expected to continue, with DanaBot email phishing campaigns to begin again this year. The attack usually relies on trojans to do their dirty work and is typically distributed in the U.S., Canada, Germany, UK, Australia, Italy, Poland, Mexico and Ukraine. As mentioned, the DanaBot malware is distributed via cracked software, where users assume they're downloading pirated copies of their favorite applications. So next time you decide to pirate something, be sure to take special precautions — or else you just may be downloading a special payload (and we're not talking about the good kind).

THI profile 3

TA551 email attack distributes IcedID malware

TA551 is an email-based malware attack that started using IcedID malware in July 2020. Before that, this attack consisted of different types of malware, such as Valak and Ursnif. But that soon changed. In the summer of 2020, the attack type switched to distributing banking trojans via email, with an aim to steal financial data from their targets.

The attackers use elusive techniques like steganography and process injection. Steganography lets hackers install malware payloads at the unoccupied portion at the end of a file, effectively hiding the banking trojan from antivirus and security software. Process injection is another technique that hackers use — often taking several forms — and with the end goal to install malware that successfully evades detection.

The attack itself looks like countless other email campaigns. It starts with an email spoofing yet another email chain, taken from a previously infected client. The email has a zip file attached, along with a message requiring a password to open the attachment. The file then opens a Microsoft Word document with macros that retrieve an installer for IcedID malware.

What you need to know:

IcedID is an information stealing malware that targets users globally, with a special emphasis on English-speaking countries. Luckily, this threat doesn't lead to ransomware or more advanced threats. However, the risk of further compromise through stolen credentials is a very real concern. Analysts should be aware of common infection chains and observables.

Hacker profile

Equation Group

Wanted for cyber warfare and digital intelligence gathering

The Equation Group is a notorious hacker collective known to use multiple remote access tools, zero-day attacks and — perhaps most notably — developed the rare capability to overwrite the firmware on hard disk drives.

The group is believed to have ties to the Tailored Access Operations (TAO) unit of the U.S. National Security Agency (NSA). TAO is believed to be a cyber warfare and digital intelligence gathering wing of the NSA.

The collective has attacks that go back to at least 2001, while others attribute hacks to the group dating back to 1998. The group's most prominent work was noticed in 2015 when it developed two types of spying malware: EquationDrug and GrayFish.

The group is also believed to be behind the Stuxnet worm, an attack that allegedly disabled the Iranian nuclear program. Last but not least, the hacking collective is suspected of collecting vulnerabilities only known to them, keeping them private so that they can eventually exploit them in future attacks.

Actor type:

Nation-state, state-sponsored

Suspected country of origin and support:

Believed to be tied to the U.S.

Motivation:

Espionage, political. The group has been linked to the NSA by some researchers.

Equation Group

Adversary vitals

Targeted sectors:

The group is known for targeting both private sector and government organizations.

- Finance
- Government
- Universities
- Energy sector
- Embassies
- Military
- Telecommunications
- Media
- Medical

Commonly exploited technologies:

- Malware
- Zero-day attacks

Weaponization:

This collective is known for building custom malware, most notably EquationDrug, GrayFish and Stuxnet

Go phish

The Cofense Phishing Defense Center (PDC)

In the name of safety, COVID-19 has taken away many things from us. But one thing it has given the world is none other than video conferencing for everyday communication.

Video conferencing has become the de facto medium to conduct business, and stay in touch with friends and family. As a result, hackers have taken notice of our increased reliance on cloud-based video conferencing and are targeting companies like Zoom in phishing campaigns.

The Cofense Phishing Defense Center (PDC) recently discovered a phishing campaign with an email impersonating official Zoom communication. Targeted accounts received an email saying Zoom had upgraded its server and that users wouldn't be able to make or join video calls without verifying their account first.

There were clear signs that the email was a spoof. The displayed header read "Zoom - no-reply@zoom[.]us" and the email was distributed via the email marketing newsletter service Constant Contact. The researchers noted the use of Constant Contact as an interesting and unique feature of this phishing attack. The attackers may have used Constant Contact thinking it could bypass certain secure email gateways (SEGs) protocols.

The phishing email then prompted users to click on an embedded URL to verify their email address. Clicking on the link redirected users to a fake Microsoft login page where they were asked to use their credentials to log in. Users were then redirected again to another spoofed Microsoft inbox. The attackers were able to harvest multiple user credentials using this attack.

Looking for trouble?

Stay ahead of current and emerging threats by subscribing to our monthly updates on threat hunting and investigation.

Subscribe Now

splunk>
turn data into doing™