MAY 2021

Threat Hunter Intelligence Report

Malware

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.

Malware 101

As technologies evolve, cyber criminals have become increasingly sophisticated. Scarier yet, the majority of cyber threats are often difficult to detect — executed by bad actors who enter your network through insidious means.

Enter malware: a threat as old as the internet. Countless types of malware exist, and unique tactics are constantly being developed. Known malware samples have already surpassed the one billion mark. And now more than ever, hackers have tools to distribute malware, reaching bigger and more diverse audiences.

In this month's issue, we'll take a look at some of the most prevalent types of malware to watch out for. We'll also cover tips for protecting your data and highlight a few other threats (and threat actors) you should know about.

Threat profile 1

Emotet

First identified in 2014 as a banking trojan targeting consumers, Emotet has reinvented itself as a persistent and pervasive threat to both the private and public sector. The Department of Homeland Security reported that Emotet is one of the most costly and destructive types of malware, costing upwards of $1 million per incident.

In 2019, Emotet attacked government agencies across France, Japan, Canada and New Zealand, and also targeted companies in the private sector, including pharmaceutical, manufacturing, technology and financial services. U.S. and European law enforcement agencies disrupted the Emotet network in February 2021, halting communications and its ability to spread. Currently, it's unclear if Emotet will remain inactive, or if it will soon resume operations.

How the attack happens: Don't be fooled — Emotet isn't as sophisticated as it sounds. This type of malware is primarily distributed through spam and phishing emails, often leading to the delivery of additional malware or attacker tools. As soon as attackers have a foothold, Emotet can capture system and user information as well as credentials, and move laterally across the network. With Emotet's worm-like features that proliferate across entire networks — as well as its use of modular libraries that help the malware evolve and adapt at a moment's notice — Emotet can be a difficult and daunting adversary to tackle.

What you need to know:

While largely inactive since all their servers were taken down, Emotet is still a great example of an incredibly destructive type of malware, especially as hackers continue to use targeted tactics to bypass email gateways and other detection methods. As a preemptive measure, be sure to provide user awareness training on common phishing themes and disabling Microsoft Office macros.

Threat profile 2

Remote access tools

Palo Alto Networks Unit 42 researchers discovered a new remote access tool (RAT) called Blackremote. First observed in September 2019, a Swedish hacker known as "Speccy" advertised Blackremote on the dark web, trying to sell it as a "full featured systems remote administration suite." It's since been used in more than 2,200 attacks with almost 50 samples.

How the attack happens: Remote access tools allow spying, backdoor administrative control and unfettered, unauthorized remote access to a target's device. Once the attackers gain control of the machine or machines in question, they can install and remove programs, hijack webcams, manipulate files, and harvest login credentials and other sensitive data. Using a RAT, hackers can also impersonate legitimate users in order to easily download additional malware, compromising other computers and devices across the network.

What you need to know:

Advertised as a legitimate tool for remote administration, Blackremote features password recovery, encryption and other "fun features" designed to prevent anti-malware software from detecting a RAT. The Blackremote manager/builder also allows users to build new client malware and control connections from infected clients.

Threat profile 3

Machete

Machete is a cyber espionage tool designed to help attackers gain a strategic edge on a political or nation-state level. Surprisingly, the famously hard-to-track collective behind Machete, APT-C-43, doesn't appear to be financially motivated. Typically distributed through social engineering and malicious websites, Machete mostly targets users in Venezuela, Columbia, Nicaragua and Ecuador.

How the attack happens: Machete malware, distributed through advanced phishing tactics, is designed to steal sensitive information — which includes user credentials, screenshots, webcam access, audio, geolocation and keylogging data. One of their most common phishing tactics is to lure users into opening a file packaged as Microsoft Office documents — primarily PowerPoint and Word.

The interface is especially convincing and can include cleverly crafted images that look totally legitimate. These crafted images and documents are often called decoy documents. Machete can then copy files to a USB device, as well as hijack the clipboard to exfiltrate data.

What you need to know:

Given the popularity of Microsoft Office for personal and commercial use, this tactic is as insidious as it is common. If you see a file in your inbox with a Microsoft Office file extension, be sure to check that it's from a trusted sender before you open it, and unleash what could potentially be malware.

Hacker profile

Stone Panda

Wanted for conspiracy to commit cyber espionage

Stone Panda — also known as APT 10 — is one of the most prolific cyber espionage groups operating today. They are known for their long-running campaign targeting managed service providers (MSPs), including infrastructure as a service (Iaas) and software as a service (SaaS) solutions. As such, companies running an MSP should prioritize the risk Stone Panda poses.

Historically, Stone Panda targets companies that boast a large amount of sensitive data, often managed on behalf of a diverse customer base.

Relentless in their pursuit, APT 10 will attack supply chains and third-party services to gain access to their targets' networks.

Stone Panda campaigned against MSPs as early as 2006 and continued all the way through 2018. Eventually, the U.S. Department of Justice (DOJ) conducted a thorough investigation into the attacks, and following the DOJ indictments, Stone Panda had no choice but to slow down their operations. However, it's doubtful they'll ever suspend operations altogether.

Actor type:

Nation-state, state-sponsored

Suspected country of origin and support:

China

Motivation:

Espionage and ideology — likely to enhance China's economic, military and technological power on the world stage.

Stone Panda

Adversary vitals

Targeted sectors:

The group is known for targeting both private sector and government organizations, specifically targets that can be of use to China's economic or military complex expansion.

- Financial services
- Healthcare
- Biotechnology
- Engineering
- Technology
- IT services
- Consulting
- Aviation
- Telecommunications

Commonly exploited technologies:

- MS Office, Outlook, Powershell, command line (cmd.exe), PsExec, Office 365
- Cloud providers (AWS, GCP, Azure), MS command line (cmd.exe)
- Remote Desktop Protocol (RDP)
- PuTTY Secure Copy Client (PSCP)

Weaponization:

Custom-built malware and open source penetration testing tools.

Tends to use "living off the land" techniques, with a mix of custom-built malware. "Living off the land" refers to using built-in OS tools to perform tasks that would normally be executed by malware, or in some other automated manner post-infection.

1

Go phish

Business email compromise

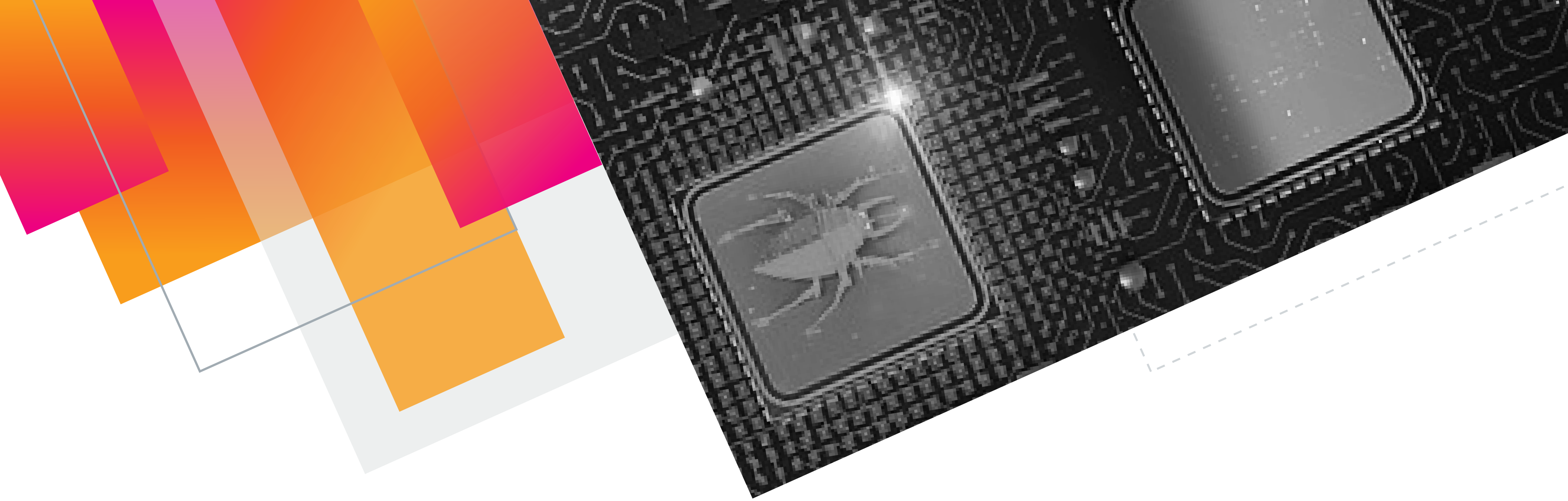
Business email compromise (BEC) is an advanced phishing technique that uses email fraud to target an organization, often with the goal of initiating fraudulent monetary transfers. According to the FBI, it's one of the most financially damaging online crimes, and one of the biggest moneymakers for cyber criminals, accounting for over half of all cyber crime losses. In Q2 2020, wire transfer losses from BEC soared by over 48% from the previous quarter to hit an average of more than $80,000, according to InfoSecurity.

A BEC attacker might compromise a real company email account and then use that account to insert themselves into corporate email communications. For example, an email that seems to come from a legitimate vendor includes an invoice with an updated mailing address, or an assistant receives an email from the CEO asking her to purchase gift cards for company employees — both were real-world BEC attacks that resulted in serious financial loss.

BEC attack: MasterMana

Security researchers at Prevailion observed a MasterMana botnet campaign that launched BEC attacks and stole credentials and cryptocurrency. MasterMana is spread through phishing emails with Microsoft Office document attachments that use macros and dynamic data exchange (DDE) exploitation to ultimately deliver either the AZORult or RevengeRAT trojans to the hapless victim. It's likely that threat actors use Word, Excel, PowerPoint and Publisher documents to deliver malicious Windows payloads in stages from multiple legitimate services including Pastebin, Bitly and Blogger.

Researchers believe financially motivated threat actors are behind the campaign due to its broad targeting of business email addresses. By using hosting services like Blogger instead of hosting their own infrastructure for malware delivery, threat actors significantly reduce costs. This campaign demonstrates that threat actors can launch long-running, successful attacks while limiting their own costs.



Looking for trouble?

We can help. Stay ahead of current and emerging threats by subscribing to our monthly updates.

Subscribe Now

splunk>®
turn data into doing™