Threat Intel Report

Prepared by:

CBI Threat Intel Group

February 8, 2022

securityalert@cbisecure.com | 800.747.8585

The close of 2021 coincided with two major security events: The Log4j vulnerability and the ransomware attack on Kronos. Organizations around the world completed a sprint to remediate Log4j, and many other organizations are still dealing with the fallout from the Kronos incident. As for threat actors, they've already moved on to what's next. Like legitimate enterprises, our cyber adversaries are keen to keep operations running. They'll continue the business of hawking breached data, infecting new systems, and exploiting new vulnerabilities that, while perhaps not as devastating as Log4j, will still have an impact on organizations around the world.

In our new monthly threat intel report, we'll keep organizations abreast of what's new on the cyber attack scene by covering emerging trends, updating on major breaches, and touching on important vulnerabilities organizations need to be aware of.

Emerging Trends

Emotet and Trickbot's New Developments

Last year, law enforcement agencies around the world worked to disrupt Emotet, one of the largest and most sophisticated botnets ever. The takedown campaign, which redirected Emotet-controlled computers to communicate with command-and-control (C&C) servers operated by law enforcement, culminated in a push of remote code that essentially forced the notorious malware to wipe itself from infected devices. But despite the success of the operation, by the end of 2021, Emotet was back.

Since its re-emergence, Emotet has only advanced in sophistication, aiding in the spread of its operations. Just as software vendors, in-house development teams, and open-source projects constantly push new releases and updates, threat actors constantly upgrade and improve malware to achieve their objectives and to keep security teams in the dark on how to detect it. Security professionals around the world have observed advancements not only in Emotet's delivery methods, but also in code obfuscation techniques aiming to prevent detection engineers from writing successful detections.

One such enhancement was observed by TrendMicro, whose researchers noticed Emotet spam campaigns attempting to evade detection by disguising the IP addresses of its C&C servers in hexadecimal and octal formats instead of the standard dotted decimal quad representation. After users have been socially engineered into opening a document and enabling macros, triggering malware execution, operating systems automatically convert the nonstandard address formats to the standard format to connect to Emotet's C&C servers.

Emotet is often used as a distributor for second stage delivery of other malware such as Trickbot, which has seen its own developments. Researchers at IBM recently had a run-in with an updated variant of TrickBot, which includes new anti-debugging measures that make it more difficult for researchers to analyze its code.

The malware uses two new tactics:

First, Trickbot's code is intentionally messy, difficult for a security analyst to understand without the use of a code-beautifying browser plugin.

Second, Trickbot looks for indications that its code has been beautified, signaling that an analyst is scrutinizing it. Upon detection of cleaner code, Trickbot sends a buffer overflow to the browser, forcing the browser to crash and making the analyst's job of code analysis that much harder.

To detect and block these threats, organizations should monitor outbound and inbound traffic, update the threat intel rules they apply to network intrusion detection devices, and leverage an endpoint detection and response solution.

Threat Actors Increasingly Target Linux Systems

2021 saw an acceleration in a trend of threat actors increasingly focusing their efforts on compromising Linux systems, and there are already indications this trend is continuing in 2022. While Windows has traditionally been the target of malicious actors, it is Linux that drives the infrastructure in the digital world, operating everything from routers and web servers to hosted applications.

Long considered by many as the most secure operating system, whether or not Linux is actually more secure, it has largely been ignored by threat actors given the much more prevalent use of Windows among the workforce. But with the continued advancement of endpoint detection technologies and other software solutions that provide visibility into Windows environments, threat actors are increasingly turning their attention to Linux.

CrowdStrike recently reported a 35% increase in the number of infections targeting their customers' Linux systems in 2021, compared to 2020. This coincides with the steady stream of security research published throughout the past year documenting not only an expansion to Linux by existing malware families, but also the development of new strains of malware that specifically target Linux.

35%

Increase in number of infections targeting Linux systems in 2021 vs 2020

Threat actors are using initial access methods such as open and insufficiently secured network ports, file drops from cloud storage, trojans, versions of common utilities and libraries, zero days such as Log4j, and even implementation weaknesses in base utilities such as cron. Linux systems are targeted for a range of objectives including establishing initial access in enterprises, accessing the valuable data that often resides in backend systems running on Linux, conducting attacks on virtualization infrastructures that leave a high "blast radius," and even using the often high-resource systems for crypto mining.

Threat actors are looking to operate more efficiently by directly hitting targets that would otherwise require lateral movement, and the fact that many Linux systems are not protected as aggressively as their Windows counterparts is driving this trend. As attackers shift an increasing portion of their efforts away from exclusively Windows orientation, IT and cybersecurity teams should ensure at least the same level of protection for Linux systems as has historically been given to Windows-based servers and endpoints.

521%

Increase in phishing attacks due to Omicon's emergence

Omicron Concerns Trigger COVID-themed Phishing Surge

Since it began grabbing news headlines two years ago, COVID-19 has provided rich fodder for threat actors in targeting companies' most important business asset: Employees. The newest variant of the virus is no exception, and Omicron has led to researchers tracking a recent uptick in phishing emails.

According to Barracuda Networks, Omicron's emergence precipitated a 521% increase in phishing attacks. For comparison, in March of 2020, the vendor observed a 667% rise in COVID-19-related phishing, and when the first vaccines became available in early 2021, its researchers noted another surge.

Now, Omicron's high transmissibility has fueled not only its own spread but also a spread in phishing lures such as offers of dubious COVID-19 tests, masks and gloves. Emails spoofing testing providers and labs have also been spotted. In another tactic, scammers send fake notifications for unpaid rapid COVID tests and ask for PayPal details to finalize the order.

Cryptocurrencies in the Crosshairs

Having been implicated in high profile attacks such as last year's crippling Colonial Pipeline attack, ransomware gangs now have targets painted on their backs, not only by the US government, but by multiple governments around the world. Due to this attention, threat actors are more likely to lay low after staging an attack, postponing the laundering of Bitcoins and waiting longer before resuming operations. They are also finding alternative means to earn money to fill this lull between ransomware campaigns.

One such means is cryptocurrencies, some of which have skyrocketed in value in recent years. Threat actors are attacking cryptocurrency at its lowest level, its investors—by stealing right from victims' crypto wallets. This practice has flourished in the past year; WeSteal and Redline Stealer are two examples of malware that can transfer crypto funds to wallets controlled by attackers.

In January, Bitdefender researchers spotted the latest offender, which they dubbed BHUNT. The malware is capable of stealing from Exodus, Electrum, Atomic, Jaxx, Ethereum, Bitcoin and Litecoin wallets, is delivered via cracked software installers, and has been distributed in the US and ten other countries across the globe.

Another attacker tactic is to exploit flaws in crypto exchanges themselves, which make the trade of cryptocurrency possible. The CEO of Crypto.com recently announced that two-factor authentication was bypassed for the accounts of 438 users, allowing attackers to withdraw over 34 million dollars' worth of digital currency. While any organization could be exploited in the same fashion, most don't yield the same payout for the level of effort required to pull off such an attack. As of now, cryptocurrency is still highly targeted by threat actors for immediate gains.

Telegram is a New Marketplace for Stolen Data

The dark web is often misconceived as a forum purely devoted to malicious activity. But just as not all websites on the dark web are malicious, not all data on the public internet is innocuous. In fact, organizations have been finding more and more of their sensitive data on the "surface web." And some of that data, according to a January Cybersixgill report, ends up for sale in the messaging app known as Telegram.

According to Cybersixgill, Telegram has become a hotspot used by cybercriminals to sell stolen financial details, organizational data, and even COVID vaccine passports to anyone. The platform's relatively loose moderation policies are one draw; the ease of setting up a Telegram channel compared with setting up and maintaining a website on the dark web is another. And because Telegram allows threat actors to easily dispose of channels and create new ones with minimal effort, criminals are difficult to track.

In short, Telegram offers privacy benefits similar to what can be found on the dark web, but without the trouble of connecting to deep web platforms. This opens up the market for threat actors to peddle data in more accessible forms to individuals who may lack the technical skills to connect to TOR.

Cyber Breach Updates

Kronos

Although the Kronos ransomware attack was disclosed more than two months ago, it is still creating chaos among multiple government, healthcare, and private organizations that utilize the vendor's solutions in payroll or contract tracking systems. To date, Kronos has only confirmed that its production environment and backups were hit, but beyond payroll issues, the full range of the incident's aftereffects are still unknown. For example, data breached in the incident could lead to sophisticated phishing attacks against employees, and partner organizations, customers, or other connected third parties may also have been affected.

Ukraine Government Sites

2017 saw one of the largest attacks to ever affect physical shipping and supply chains when the NotPetya ransomware was introduced into a tax preparation software popular in Ukraine. With its swift, uncontrolled spread around the globe, companies realized that in our interconnected world, the problems experienced in a country across the globe can adversely affect business.

In January, Ukraine saw another politically motivated attack, this one affecting the websites of at least 70 government organizations. According to Ukranian cyber security organizations, attackers abused a vulnerability in a web content management system and exploited the Log4j flaw. Although this attack did not have the widespread global effect of NotPetya, it prompted a warning from CISA advising organizations to take steps to improve cyber resilience and to be aware of Russian state-sponsored cyber threats. Organizations must also be aware of their connections with third-party suppliers whose products and services contribute to operations.

70

Government organizations' websites were effected by the Log4j vulnerability

Vulnerabilities

McAfee

McAfee has responded to CVE-2022-0166, a high-severity vulnerability that resides in McAfee Enterprise Agents for Windows, particularly the McAfee ePolicy Orchestrator (McAfee ePO). The policy enforces what the device and users can and cannot do from an enterprise standpoint. In versions 5.7.5 and prior, it allows an unprivileged user with local access to escalate their access to NT AUTHORITY\SYSTEM privileges. McAfee reported that the unprivileged user could place a new openssl.cnf in the location of the agent to exploit this vulnerability.

Cisco

Cisco pushed out a major update to the Cisco ASR 5000 series of devices, which are designed to operate virtual mobile networks for enterprises and service providers. The update provides fixes for CVE-2022-20649, an RCE vulnerability in its Redundancy Configuration Manager. The Cisco Alert states that the bug exists because the debug mode is incorrectly enabled for specific services, allowing threat actors to connect to the device and escalate privileges once they enable debug mode.

Contact the CBI Threat Intel Group at securityalert@cbisecure.com

Sources

Emotet

https://thehackernews.com/2022/01/emotet-now-using-unconventional-ip.html
https://gbhackers.com/emotet-uses-unconventional-ip-address-formats-to-spread-malware/
https://www.trendmicro.com/en_no/research/22/a/emotet-spam-abuses-unconventional-ip-address-formats-spread-malware.html

Trickbot

https://threatpost.com/trickbot-crash-security-researchers-browsers/178046/
https://securityintelligence.com/posts/trickbot-bolsters-layered-defenses-prevent-injection/
https://www.darkreading.com/vulnerabilities-threats/trickbot-injections-get-harder-to-detect-analyze

Linux Systems

https://iemlabs.com/malware-targeting-linux-systems-grows-by-35-in-2021/
https://www.crowdstrike.com/blog/linux-targeted-malware-increased-by-35-percent-in-2021/

COVID Phishing

https://www.helpnetsecurity.com/2022/01/24/covid-test-scam-emails/
https://www.infosecurity-magazine.com/news/covid19-phishing-surge-500-omicron/
https://www.ociso.ucla.edu/resources/covid-19-cybersecurity/covid-19-scams-phishing-malware-ransomware

Cryptocurrencies

https://www.bitdefender.com/blog/labs/poking-holes-in-crypto-wallets-a-short-analysis-of-bhunt-stealer/
https://indianexpress.com/article/technology/crypto/new-bhunt-malware-targets-your-crypto-wallets-and-passwords-7736926/
https://news.bitcoin.com/new-bhunt-malware-targets-cryptocurrency-wallets-via-software-installs/
https://www.thehindubusinessline.com/info-tech/targeted-cyberattacks-on-cryptocurrency-industry-to-rise-in-2022-report/article37733880.ece

Telegram

https://www.bleepingcomputer.com/news/security/telegram-is-a-hotspot-for-the-sale-of-stolen-financial-accounts/
https://www.cybersixgill.com/blog/telegram-a-cybercriminal-hotspot-compromised-financial-accounts/

Ukraine

https://www.securityweek.com/ukraine-attacks-involved-exploitation-log4j-october-cms-vulnerabilities
https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped

McAfee

https://kc.mcafee.com/corporate/index?page=content&id=SB10378
https://www.cisa.gov/uscert/ncas/current-activity/2022/01/21/mcafee-releases-security-update-mcafee-agent-windows
https://threatpost.com/mcafee-bug-windows-system-privileges/177857/

Cisco

https://thehackernews.com/2022/01/cisco-issues-patch-for-critical-rce.html
https://www.securityweek.com/cisco-patches-critical-vulnerability-rcm-staros
https://www.systemtek.co.uk/2022/01/cisco-redundancy-configuration-manager-for-cisco-staros-software-multiple-vulnerabilities-cve-2022-20648-cve-2022-20649/