MAY EDITION 2022

THE THINGS YOU SHOULD KNOW

RESEARCHERS EXPOSE INNER WORKINGS OF BILLION-DOLLAR WIZARD SPIDER CYBERCRIME GANG

The Wizard Spider has been exposed, shedding light on its organizational structure and motivations.

"Most of Wizard Spider's efforts go into hacking European and US businesses, with a special cracking tool used by some of their attackers to breach high-value targets," Swiss cybersecurity company PRODAFT. Wizard Spider, also known as Gold Blackburn, is believed to operate out of Russia and refers to a financially motivated threat actor linked to the TrickBot botnet. This modular malware was officially discontinued earlier this year despite improved malware like BazarBackdoor.

That's not all. The TrickBot operators have also extensively cooperated with Conti, another Russia-linked cybercrime group notorious for offering ransomware-as-a-service packages to its affiliates.

Gold Ulrick (aka Grim Spider), the group responsible for distributing the Conti (previously Ryuk) ransomware, has historically leveraged initial access provided by TrickBot to deploy the ransomware against targeted networks.

"Gold Ulrick is composed of some or all of the same operators as Gold Blackburn, the threat group responsible for the distribution of malware such as TrickBot, BazarLoader and Beur Loader," cybersecurity firm Secureworks notes in a profile of the cybercriminal syndicate. Typical attack chains involving the group commence with spam campaigns that distribute malware such as Qakbot (aka QBot) and SystemC, using them as launchpads to drop additional tools, including Cobalt Strike, for lateral movement before executing the locker software.

In addition to leveraging a wealth of utilities for credential theft and surveillance, Wizard Spider is known to use an exploitation toolkit that takes advantage of known security vulnerabilities such as Log4Shell to gain an initial foothold into victim networks.

Also put to use is a cracking station that hosts cracked hashes associated with domain credentials, Kerberos tickets, and KeePass files, among others.

MICROSOFT WARNS OF "CRYWARE" INFO-STEALING MALWARE TARGETING CRYPTO WALLETS

Microsoft is warning of an emerging threat targeting internet-connected cryptocurrency wallets, signalling a departure in using digital coins in cyberattacks.

The tech giant dubbed the new threat "cryware," with the attacks resulting in the irreversible theft of virtual currencies through fraudulent transfers to an adversary-controlled wallet.

"Cryware is an information stealer that collects and exfiltrated data directly from non-custodial cryptocurrency wallets, also known as hot wallets," Berman Enconado and Laurie Kirk of the Microsoft 365 Defender Research Team disclosed in a new report.

"Because hot wallets, unlike custodial wallets, are stored locally on a device and provide easier access to cryptographic keys needed to perform transactions, more and more threats are targeting them."

Attacks of this kind are not theoretical. Earlier this year, Kaspersky disclosed a financially-motivated campaign staged by the North Korea-based Lazarus Group,

targeting crypto companies with malware designed to drain funds out of hot wallets.

MEDICAL DOCTOR CHARGED WITH CREATING THE THANOS RANSOMWARE BUILDER

A cardiologist turned alleged malware developer has been charged with creating the Thanos ransomware builder.

According to a US criminal complaint, Moises Luis Zagala Gonzalez, 55, a citizen of France and Venezuela who resides in Ciudad Bolivar, Venezuela, engaged in attempted computer intrusions and conspiracy to commit computer intrusions.

Zagala is alleged to have both sold and leased ransomware packages he developed to cybercriminals.

According to US prosecutors, he is also accused of training would-be attackers on how to use his wares to extort victims and subsequently boasted about successful attacks.

'ETERNITY MALWARE' OFFERS SWISS ARMY KNIFE OF CYBERCRIME TOOLS

Collectively named the 'Eternity Project' by its architects, the suite of malware already includes stealers, clippers, worms, miners, and ransomware, with a Distributed Denial of Service (DDoS) bot apparently under development.

A Telegram channel provides information about forthcoming software updates and videos documenting the malware's functionality to hundreds of subscribers.

Eternity Stealer

The developer sells the Stealer module for $260 as an annual subscription. The Eternity Stealer steals passwords, cookies, credit cards, and crypto-wallets from the victim's machine and sends them to the TA's Telegram Bot.

The features of the stealer malware mentioned on the TAs website and Telegram channel are:

• Browsers collection (Passwords, CreditCards, Cookies, AutoFill, Tokens, History, Bookmarks)

• Chrome, Firefox, Edge, Opera, Chromium, Vivaldi, IE, and +20 more.

• Email clients: Thunderbird, Outlook, FoxMail, PostBox, MailBird.

• Messengers: Telegram, Discord, WhatsApp, Signal, Pidgin, RamBox.

• Cold cryptocurrency wallets: Atomic, Binance, Coinomi, Electrum, Exodus, Guarda, Jaxx, Wasabi, Zcash, BitcoinCore, DashCore, DogeCore, LiteCore, MoneroCore.

• Browser cryptocurrency extensions: MetaMask, BinanceChain, Coinbase Wallet, and 30+ more.

• Password managers: KeePass, NordPass, LastPass, BitWarden, 1Password, RoboForm and 10+ more.

• VPN clients: WindscribeVPN, NordVPN, EarthVPN, ProtonVPN, OpenVPN, AzireVPN.

• FTP clients: FileZilla, CoreFTP, WinSCP, Snowflake, CyberDuck.

• Gaming software: Steam session, Twitch, OBS broadcasting keys.

• System credentials: Credman passwords, Vault passwords, Networks passwords).

CYBERSECURITY BREACH BY MILITARY OFFICIALS ON WHATSAPP SAID TO BE UNEARTHED IN INDIA, HIGH-LEVEL PROBE UNDERWAY: REPORT

Intelligence agencies have unearthed a cybersecurity breach by military officials, which is suspected to be linked to espionage-related activities by a neighboring country.

Responding to an ANI query on the cybersecurity breach issue, defense sources said: "The military and intelligence agencies have unearthed a cybersecurity breach by some military officials, which is likely to be linked to espionage-related activities by a neighboring country."

On the issue of action being taken against the officials facing allegations, the sources said, "An inquiry, which has been promptly ordered, is in progress. Acts of infringements to existing orders, especially involving counterintelligence matters, by military officials, are dealt with the strictest possible manner, as they are subject to Official Secrets Act."

The sources said that the strictest possible action would be taken against all the officials found guilty in the ongoing investigations.

"In recent times, suspected Pakistani and Chinese intelligence operatives have been attempting to engage with military personnel on social media platforms to

gain sensitive information on the military and its activities."

Even though most of their attempts fail, they have been able to extract information from some of the military personnel who fall into their trap.

UNDERSTANDING MALWARE

Malware discussion typically encompasses three main aspects:

• Objective: What the malware is designed to achieve

• Delivery: How the malware is delivered to the target

• Concealment: How the malware avoids detection (this item is beyond the scope of this discussion)

Things to observe in malware.

OBJECTIVES

Malware is created with an objective in mind. While it could be said that the aim is "limited only to the imagination of its creator," this will focus on some of the most common objectives observed in malware.

Exfiltrate Information

Stealing data, credentials, payment information, etc., is a recurring theme in cybercrime. Malware focused on this type of theft can be extremely costly to a person, company, or government target that falls victim.

Disrupt Operations

Actively working to "cause problems" for a target's operation is another objective seen in malware. From a virus on a single computer corrupting critical OS files (making that one system unusable) to an orchestrated, physical self-destruction of many systems in an installation, the level of "disruption" can vary. And there's also the scenario where infected systems are directed to carry out large-scale distributed denial of service (DDOS) attacks.

Ransomware

Some malware is focused on directly extorting money from the target. Scareware uses empty threats (ones which are unsubstantiated and couldn't be carried out) to "scare" the target into paying some money. Ransomware is malware that attempts to prevent a target from accessing their data (usually by encrypting files on the target) until the target "pays up." While there is debate over whether ransomware victims should or should not pay, it has become enough of a threat that some companies have preemptively purchased Bitcoin just in case they get hit with ransomware and decide to pay the ransom.

Types of malware attack vectors

The three main types of malware attack vectors:

• Trojan Horse: This program appears to be one thing (e.g. a game, a practical application, etc.) but is a delivery mechanism for malware. A trojan horse relies on the user to download it (usually from the internet or via email attachment) and run it on the target.

• Virus: A virus is a type of self-propagating malware which infects other programs/files (or even parts of the operating system and/or hard drive) of a target via code injection. This behavior of malware propagation through injecting itself into existing software/data is a differentiator between a virus and a trojan horse (which has purposely built malware into one specific application and does not attempt to infect others).

• Worm: Malware designed to propagate itself into other systems is a worm. While virus and trojan horse malware are localized to one infected target system, a worm actively works to infect other targets (sometimes without interaction on the user's behalf).

Over the years, malware has been observed to use various delivery mechanisms or attack vectors. While a few are admittedly academic, many attack vectors effectively compromise their targets. These attack vectors generally occur over electronic communications such as email, text, vulnerable network service, or compromised websites. Malware delivery can also be achieved via physical media (e.g. USB thumb drive, CD/DVD, etc.).

Ensure Your Network is Secure

Controlling access to systems on your organization's network is an excellent idea. Using proven technology and methodologies—such as using a firewall, IPS, IDS, and remote access only through VPN—will help minimize the attack "surface" your organization exposes. Physical system isolation is usually considered an extreme measure for most organizations and is still vulnerable to some attack vectors.

Perform Regular Website Security Audits

Scanning your organization's websites regularly for vulnerabilities (i.e. software with known bugs, server/service/application misconfiguration) and detecting if known malware has been installed can keep your organization secure, protect your users, and protect customers and visitors to public-facing sites.

Create Regular, Verified Backups

Having a regular (i.e. current and automated) offline backup can be the difference between smoothly recovering from a destructive virus or ransomware attack and stressful, frantic scrambling with costly downtime/data loss. The key here is to have regular backups that are verified to be happening on the expected regular basis and are usable for restore operations. Old and outdated backups are less valuable than recent ones, and backups that don't restore properly are of no value.

In summary

Malware takes on many different forms and attacks in different ways. But with some thoughtful preparation, process improvements, and ongoing user education, your organization can gain and maintain a solid security stance against malware attacks.