Edition 190

22nd August 2022

by Richard Beck

$2 billion worth of cryptocurrency stolen so far in 2022

Hackers have already stolen nearly $2 billion worth of cryptocurrency in 2022 — and the year is only half over. As of July, $1.9 billion in crypto has been stolen by cybercriminal hacks, according to Chainalysis' "Mid-year Crypto Crime Update." At this point last year, hackers had stolen $1.2 billion, according to the report. That's a spike of nearly 60% compared to a year ago. Bad actors are increasingly targeting decentralized finance (DeFi) protocols, which are uniquely vulnerable to hacking, according to the report. DeFi programs are the underlying blockchain technology that enable financial transactions to occur outside of traditional banks. These programs primarily utilize the Ethereum blockchain. DeFi programs are public and use open-source code, which can be helpful because it typically allows for security issues to be discovered and fixed quickly. However, since open-source code is available for anyone to review, cybercriminals are able to extensively study the code and find vulnerabilities that can be exploited and used to steal crypto funds, according to the report.

There are plenty of virtual wallets that can safely store your crypto and secure it against online attacks. However, it's important to do thorough research first to determine which type of wallet makes sense for you. It's also crucial to do your

own research before investing in anything to avoid potential scams. Additionally, law enforcement must continue to develop its ability to seize stolen cryptocurrency so that hacks are no longer attractive to cybercriminals, Chainalysis reports. Although many investors are drawn to the unregulated nature of cryptocurrency, the lack of a central regulating authority means investors typically don't have the same protections offered by traditional financial institutions like banks. And remember, crypto assets can be highly volatile and subject to wild price valuations. There's no guarantee of making a return on your investment, which is why experts recommend only investing as much as you're prepared to potentially lose. Edited – Original Source: Chainalysis

Continued Russian cyber-attacks on Ukraine

Russian cyber-attacks against systems in Ukraine, as part of the former's ongoing invasion attempt, have been almost entirely the work of government-backed intelligence and military agencies. This is according to a report from security vendor Trustwave, which said that known threat groups from the Russian Federal Security Service (FSB), Foreign Intelligence Service (SVR), and the Main Directorate of the General Staff of the Armed Forces (GRU) are responsible for most attacks against both critical industrial infrastructure and data networks in Ukraine. Cyber-attacks against public and private sector organizations in Ukraine have increased dramatically since Russia invaded the country in late February.

Researchers from Trustwave's SpiderLabs operation say notorious groups such as APT29, also known as "Fancy Bear," and APT28, or "Cozy Bear," are among the nation-state crews that have been breaking into Ukrainian networks and attempting to disrupt or even destroy vulnerable systems. Citing both its own research as well as accounts from European government agencies and other cybersecurity vendors like CrowdStrike and SentinelOne, the Trustwave team outlined a bevy of attacks and malware samples that can all be tied back to Kremlin-backed hacking groups. The attacks included a variety of data wipers, DDoS attacks and a multi-layered operation that disrupted satellite internet provider Viasat. The report casts doubt on the prospect that the Russian government has been enlisting help from the private hacking sector, as had first been speculated. Rather than trying to enlist or conscript ordinary cybercriminals to do their dirty work, decision-makers in the Kremlin have opted to keep virtually everything in-house and use personnel from its intelligence and military units to carry out attacks. The decision to use government agencies rather than enlist the aid of Russian cybercrime groups was likely due to the sophistication and preparation of the FSB- and GRU-backed hacking crews.

Trustwave's report found the Russian cyber-attacks were largely intended to disrupt the normal operation of critical infrastructure, such as energy plants, or create havoc by wiping the data from servers on essential networks. A third category of attacks, meanwhile, focused on intelligence gathering and espionage activity by covertly installing spyware on endpoint systems. Trustwave found that, apart from the customized ICS malware, nearly all the malware samples in use were previously known hacking tools. The most significant modifications were small changes to the binaries that would allow them to temporarily evade antimalware products. The aim of the attacks has evolved over the course of the war. Sigler explained that as the Ukraine conflict drags on far longer than the

Kremlin anticipated, the tactics of Russian hackers have changed from all-out destruction with wiper tools to information and intelligence gathering. Edited – Original Source: Trustwave

Malware on USB drive capable of disrupting Industrial Control Systems (ICS)

A significant percentage of the malware seen last year on USB drives used in industrial facilities could target and disrupt industrial control systems (ICS), according to a report published this week by Honeywell. The industrial giant has published its fourth annual report focusing on the malware found by one of its dedicated security products on the USB drives that were brought into its customers' industrial environments. Honeywell's analysis of the data found that the percentage of industrial-specific malware has increased to 32%, from 30% in the 2021 report and 11% in the 2020 report. The percentage of malware designed to propagate over USB or to specifically exploit USB for infection increased to 52%, significantly higher than the 37% seen in 2021.

"USB-borne malware is clearly being leveraged as part of larger cyber-attack campaigns against industrial targets. Adaptations have occurred to take advantage of leveraging the ability of USB removable media to circumvent network defences and bypass the air gaps upon which many of these facilities depend on for protection. Continued diligence is necessary to defend against the growing USB threat, and strong USB security controls are highly recommended," Honeywell concluded.

There has also been a slight increase in malware that can cause disruption to operational technology (OT) systems — this includes loss of control or loss of view. Specifically, 81% of the malware detected by Honeywell's product on USB drives was disruptive, up from 79% in 2021. The company found that more than three-quarters of the malware were trojans, and 51% — the same as in the previous year — provided remote access or remote-control capabilities. Edited – Original Source: Honeywell

Cloud and Web Attack Vulnerabilities Exposed

Many organizations are struggling to adequately protect the cloud environments implemented during the pandemic and adapt their comprehensive cybersecurity strategy to evolving threats. The data comes from a joint research report by the Cloud Security Alliance (CSA) and Proofpoint, which queried more than 950 IT and security professionals at organizations of different sizes and in various locations across the Americas, EMEA and APAC. Dubbed the "Cloud and Web Attacks" study, the report suggests that while many companies substantially accelerated their digital transformation to adapt to a remote workforce during the pandemic, the speed of the transition presented unintended consequences, mainly due to the large-scale structural changes required.

Fast forward to the present day, Proofpoint said risks and threats through the supply chain continue to increase as organizations migrate to the cloud and increasingly rely on third parties and partners. In terms of primary cloud and web security objectives for 2022, 43% of organizations cited protecting customer data, while 41% mentioned automating cloud and web threat prevention solutions as

their number one priority. The Proofpoint study also analysed the perception of responders in relation to the main vulnerability point in cloud and web applications. While 47% of those surveyed blame dealing with legacy systems as their number one security problem, more of them (49%) agreed that the main source of risks to security are still users of the enterprise IT systems. To protect themselves against cloud and web threats, organizations say they most commonly use security awareness training. Edited – Original Source: Proofpoint

Malicious PyPi packages turn Discord into password-stealing malware

A dozen malicious PyPi packages have been discovered installing malware that modifies the Discord client to become an information-sealing backdoor and stealing data from web browsers and Roblox. The twelve packages were uploaded to the Python Package Index (PyPI) on August 1, 2022, by a user named "scarycoder," and discovered by researchers at Snyk. Contrary to the common typo-squatting approach, these packages use their own names and promise various features to promote themselves to interested developers. The Python packages pretend to be Roblox tools, thread management, and basic hacking modules, but none feature the promised functionality. Instead, the packages install password-stealing malware on developers' devices. Unfortunately, this malicious set of PyPi Python packages has not been removed from the open-source package repository at the time of writing this, so software developers are still at risk.

Kaspersky also published a report where it presented two other PyPi packages that contain info-stealing malware and modify the Discord client as well. The stealers in those packages focus on collecting account credentials from cryptocurrency wallets, Steam, and Minecraft, while an injected script monitors for inputs like email addresses, passwords, and billing information. After this step, the stealer scans the host's Downloads, Documents, and Desktop folders to locate 2FA recovery lists, password text files, Discord tokens, Paypal account info, and more. Edited – Original Source: Synk

Cisco announce high-severity vulnerability patch

Cisco has announced patches for a high-severity escalation of privilege vulnerability in AsyncOS for Cisco Secure Web Appliance. Formerly Web Security Appliance (WSA), Cisco's Secure Web Appliance is an enterprise protection solution designed to block risky sites and provide application visibility and control. Tracked as CVE-2022-20871, the newly addressed flaw can be exploited remotely to inject commands and escalate privileges to root, but requires authentication for successful exploitation. According to Cisco, the security bug exists because user-supplied input for the web interface is not sufficiently validated.

"An attacker could exploit this vulnerability by authenticating to the system and sending a crafted HTTP packet to the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root," Cisco explains.

The tech giant also notes that the attacker needs to have at least read-only credentials to successfully exploit the issue. Cisco has resolved the vulnerability

with the release of AsyncOS for Secure Web Appliance version 14.5.0-537 and plans to release updates for versions 12.5 and 14.0 of the appliance as well. There are no workarounds available to address the vulnerability and Cisco encourages customers to install the available patches as soon as possible. Cisco says it is not aware of this vulnerability being exploited in malicious attacks. Edited – Original Source: Cisco

2 million + Android users downloaded malicious apps

Over two million Android users have downloaded a series of malicious apps that bypassed security protections to get into the Google Play app store, researchers have warned. After installation, the apps use sneaky techniques to hide themselves from the user to avoid being removed, while serving up malicious ads that can link directly to malware. A total of 35 "clearly malicious" apps in the Google Play store have been discovered and detailed by cybersecurity researchers at Bitdefender, many of which duped victims into downloading them. If users have downloaded any of the apps, it's recommended they find and delete them immediately. It's common for malware-laden apps to look clean enough to bypass app store protections, because they only connect to the servers where they receive the malicious download after they have been installed on the user's device.

One of the apps discovered by researchers is called GPS Location Maps, and it's been downloaded by over 100,000 users. According to researchers, after being downloaded the app changes its label from 'GPS Location Maps' to 'Settings' to make it difficult to find and remove, while it serves pop-up ads linking to malicious websites. This, and many of the other dangerous apps identified by Bitdefender, also gain permission to display over the top of other apps in attempts to force the user to click through. Some of the apps also simulate user clicks to click through to adverts, helping them create illicit profits from enforced visits. Those behind the GPS Location Maps have put a lot of effort into ensuring the malicious app is difficult to reverse engineer and examine, with the main Java payload hidden inside encrypted files. Even when the files are decrypted, the code remains obfuscated.

The malicious app also uses another technique to stay hidden – it doesn't appear in the list of most recently used apps on Android devices. Each of the malicious apps is listed as the only app published by a single developer, but their email addresses and websites are all very similar, leading Bitdefender to believe all of the apps could be the work of a single group or individual. Other apps that have been downloaded more than 100,000 times include Personality Charging Show, Image Warp Camera and Animated Sticker Finder. Users should always be careful about what they download and be particularly wary of apps by unknown developers which have large numbers of downloads but no reviews. Edited – Original Source: Bitdefender