INDIA FUTURE FOUNDATION

INDIA FUTURE FOUNDATION

Freedom of Expression, Trust and Safety on Internet

LOCKBIT 2.0 RANSOMWARE PROLIFERATES

The Lockbit Ransomware-as-a-Service (RaaS) gang is active since 2019. The ransomware now ramped up its targeted attacks. Like Darkside and Revil, the ransomware gang offers a platform. The ransomware gang recently targeted Accenture. The group claims that Lockbit 2.0 is one of the fastest ransomware variants. The new version includes automatic encryption of devices in the Windows network, and to achieve that, Lockbit abuses the Active Directory group policies. Lockbit is similar to LockerGoga and MegaCortex malware as it shares similar Tactics, Techniques and Procedures (TTPs). Once a single device is compromised, Lockbit can scan the whole network and tries compromise other devices.

OTHER STORIES INSIDE THIS ISSUE:

The malware gang makes it difficult for endpoint security tools to detect the ransomware by using native tools and protocols of Windows. The Lockbit 2.0 is capable of exfiltrating valuable information before encrypting the devices. The stolen data gives the malware gang an additional edge if the companies hit refuses to pay the ransom or decrypts their files, the malware gang can sell the data to competitors or disclose the information publicly.

The Lockbit ransomware gang is reportedly recruiting insiders to compromise their targets and promises to pay millions in dollars. The malware authors provide a StealBit trojan variant to automatically exfiltrate data. The ransomware uses state-of-the-art techniques, and the victims of Lockbit ranges across multiple sectors.

Source:https://threatpost.com/lockbit-ransomware-proliferates-globally/168746/

PIRACY SITES MAKE MORE THAN $1.3 BILLION FROM MALICIOUS AND REAL ADS

Piracy is a major problem for content creators as it directly causes harm to the income. Now piracy is not only a problem for legitimate content creators but also for the people who use these sites and are exposed to cyber attacks. Pirated websites are key sources of malware and ransomware. A study reveals how these pirated websites make over $1.3 billion dollars a year from advertising. Many of these pirated websites frequently change domains to avoid enforcement and blocklists. Law enforcement agencies identified at least 84000 illicit streaming sites.

The business of illegal digital market boomed in the Covid-19 pandemic as people watched content over the web.Combating the ad-driven piracy requires collective efforts of law enforcement agencies, advertisement companies, and government regulators. The advertising ecosystem hire intermediaries to promote their ads on websites and applications. Pirate operators used the unaware Ad Tech companies to advertise the ads on their platforms. Major brands accounted for about 4% of the advertising on the pirate websites and 24% of the ads on pirate apps.

Source: https://therecord.media/piracy-sites-make-more-than-1-3-billion-from-malicious-and-real-ads/

MOZI IOT BOTNET EVOLVES AND GAINS ABILITY TO TAMPER WEB TRAFFIC

The Mozi botnet that targeted IoT devices and routers now ramped up its capabilities and tampers with web traffic of compromised systems. The botnet leverages techniques such as DNS spoofing and HTTP session hijacking to direct users to malicious websites. The botnet malware recently started targeting network gateway equipment manufactured by Netgear, Huawei, and ZTE. Microsoft said, "Network gateways are a particularly juicy target for adversaries because they are ideal as initial access points to corporate networks.

By infecting routers, [Mozi] can perform man-in-the-middle (MITM) attacks —via HTTP hijacking and DNS spoofing—to compromise endpoints and deploy ransomware or cause safety incidents in OT facilities". Mozi appeared for the first time in December 2019 and exploited default remote access passwords and unpatched vulnerabilities. The botnet is famous for DoS attacks, data exfiltration, and payload execution. A report analyzed that the Mozi accounted for nearly 90% of IoT network traffic, and the IoT based attacks increased nearly 400% from the previous two years.

Source: https://therecord.media/mozi-botnet-gains-the-ability-to-tamper-with-its-victims-traffic/

CITRIX VULNERABILITY LEADS TO US CENSUS BUREAU BREACH

Malicious actors exploited a Citrix ADC zero-day vulnerability to breach the US Census Bureau servers. The attackers, after breaching the server, set up rogue admin accounts that allowed them to execute malicious code remotely but could not install backdoors to maintain access to the servers. The vulnerability exploited is the CVE-2019-19781, a critical bug in Citrix's Application Delivery Controller (ADC), Gateway, and SD-WAN WANOP appliances. When exploited successfully, the vulnerability allows the remote attackers to execute arbitrary code on unpatched servers.

It even allowed attackers to gain access to an organization's internal network without requiring authentication. Citrix, after discovering the vulnerability, published a security advisory of immediate mitigation steps while the company worked on the security patch to fix the vulnerability.

Before the security fix arrived, malicious attackers started attacking the Citrix ADC devices, and the US Census Bureau's servers appear to be among the first systems that are compromised. Due to lack of logging, in-depth logs are rotated or deleted from the compromised systems. According to a report, the Citrix vulnerability is one of the most exploited vulnerabilities over the past two years.

Source: https://www.bleepingcomputer.com/news/security/us-census-bureau-hacked-in-january-2020-using-citrix-exploit/

NEW ADLOAD VARIANT BYPASSES APPLE SECURITY

A new wave of attacks involves a notorious macOS adware family identifies as an Adload variant that remained undetected by Apple's security checks. Researchers detected more than 150 unique samples in the wild in 2021 alone. Some of these even evaded Apple's on-device malware scanner – Xprotect. Although XProtect provides security against older Adload variants, the malicious software continuously adapts and evades detection. The adload is targetting macOS since 2017.

The adload is capable of backdooring an affected system and install potentially unwanted programs (PUPs) and transmit a large amount of user information. The 2021 version of AdLoad uses different file extension patterns like .system or .service to bypass the security solutions. The malware installs a persistence agent and deploys malicious droppers that impersonate as a fake Player.app to install malware. The malicious droppers are digitally signed using developer certificates. Apple addressed a zero-day vulnerability tracked by CVE-2021-30657 and deployed that allowed unapproved software on the compromised systems.

Source: https://thehackernews.com/2021/08/new-adload-variant-bypasses-apples.html

SECURELY USING WIRELESS DEVICES IN PUBLIC SETTINGS

Most wireless device users are not aware of the basic security hygiene, and the convenience of wireless devices vastly overshadows the need for security. This results in a number of cyberattacks. Cyber-attacks have increased in the Covid-19 pandemic. Protecting personal and corporate data is now a challenge, especially in public networks. The NSA recently published official guidance to protect mobile devices in public settings. Below are some key insights of NSA's key Do's and Don't for Wireless Device Security:

- Disable Wi-Fi, Bluetooth, and other NFC services on mobile devices when not in use.
- Restart the devices after using untrusted wireless connections, and delete unused networks from the wireless settings.
- Disable Wi-Fi auto-connect and only connect to networks with WPA2-encryption.
- Use Multi-Factor Authentication whenever possible, which can help with the defence against password hash captures.
- Use an access list that can allow or deny applications/devices that can use your device's Bluetooth connection.
- Use an IPsec VPN and HTTPS browsing protocols.
- When using public networks, avoid accessing sensitive personal or company data and try to avoid bank transactions.
- Avoid plugging mobile devices into public USB charging stations, including those found in airports and shopping centres.
- For laptops, do not browse the web using the administrator account.
- Avoid using Bluetooth to communicate passwords or sensitive data.
- Do not set public Wi-Fi networks to be trusted networks.

NORTH-KOREAN APT EXPLOITS MICROSOFT INTERNET EXPLORER

The North-Korean APT group – InkySquid or APT7 or ScarFruit compromised a South Korean newspaper into a watering hole attack. The attackers used Bluelight malware and exploited Internet Explorer vulnerability. Researchers reported, "As with the initial redirect, the attacker chose to bury their malicious code amongst legitimate code. In this case, the attacker used the 'bPopUp' JavaScript library alongside their own code." As the code is largely legitimate, it is a challenge for detection solutions to detect the malicious code.

Researchers highlighted that the BlueLight appears to be delivered as a secondary payload, and Cobalt Strike is the primary payload. The C2 server used different cloud providers for its operations like exfiltration of data, username and IP addresses, OS version and more. Researchers said, "The main C2 loop starts after the initial upload of the reconnaissance data, iterating once every approximately 30 seconds. For the first five minutes, each iteration will capture a screenshot of the display and upload it to the 'normal' subdirectory with an encoded timestamp as the filename. After the first five minutes, the screenshot uploads once every five minutes."

Source: https://threatpost.com/inkysquid-exploiting-ie-bugs/168833/

CYBERCRIME GROUP ASKS EMPLOYEES TO DEPLOY RANSOMWARE

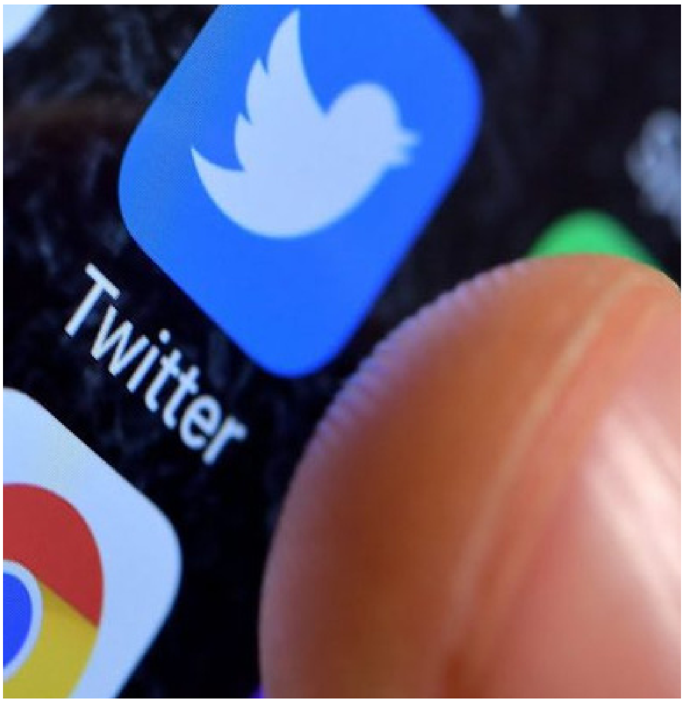
Nigerian threat actors are reportedly attempting to recruit employees to deploy Black Kingdom ransomware on corporate networks and offering the employees $1 million in bitcoins. The threat actors offer the employees a cut from the ransom profits. Black Kingdom ransomware is also referred to as DemonWare and DEMON. The Nigerian ransomware group previously targeted Microsoft Exchange's ProxyLogon vulnerabilities tracked by CVE-2021-27065. The actors send out an initial email to employees to install ransomware and offer a payment.

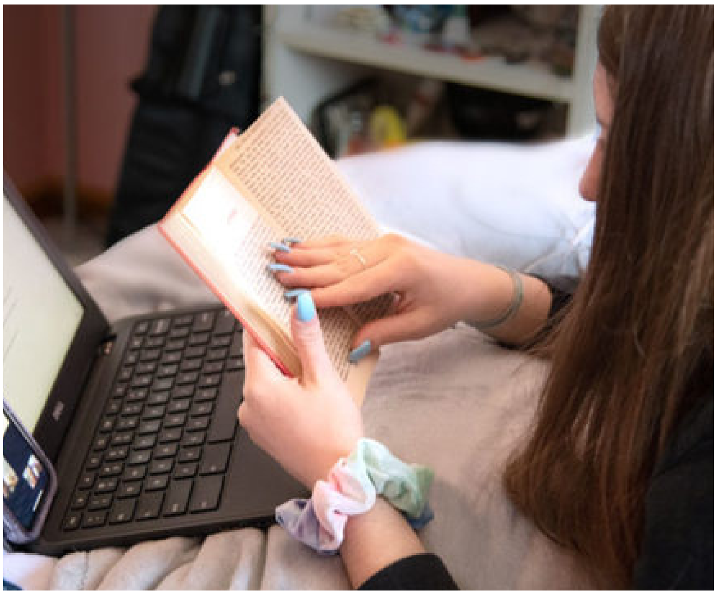
The threat actors tell the employees that they can either launch the ransomware physically or remotely. Researchers engaged with the threat actors to better understand their motivations and tactics. The threat actors used Outlook or Telegram to contact the researchers and shared executable file links using file-sharing websites WeTransfer or Mega.nz. Researchers highlighted that the executable file shared is ransomware and is named "Walletconnect (1).exe". Based on the conversation, researchers noted that the actors are likely to be Nigerian. The threat actors used LinkedIn to collect corporate email addresses.

Source: https://thehackernews.com/2021/08/cybercrime-group-asking-insiders-for.html

KASEYA FIXES TWO NEW ZERO-DAY VULNERABILITY

Kaseya released a security update to address server-side Kaseya Unitrends zero-day vulnerabilities found by security researchers at the Dutch Institute for Vulnerability Disclosure (DIVD). The DIVD released a knowledge base article with steps to mitigate the vulnerability. The vulnerabilities affected Kaseya's Unitrends enterprise backup and continuity solution. The zero-day vulnerability is capable of privilege escalation and authenticated remote code execution.





After releasing the fixes, Kaseya reached out to customers to patch vulnerable servers and apply client mitigations to safeguard against the identified zero-day attack. Unlike the Kaseya ransomware attack, these vulnerabilities are harder to exploit as attackers need valid credentials to launch the attack or need a low privilege account in order to escalate privileges on the unpatched Unitrends servers.

INDIA FUTURE FOUNDATION

India Future Foundation
Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com
BSMT, Building no. 2731 EP, Sector 57, Golf Course Ext. Road, Gurugram,
Haryana, India – 122003
www.indiafuturefoundation.com