Payatu

August 2023

Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

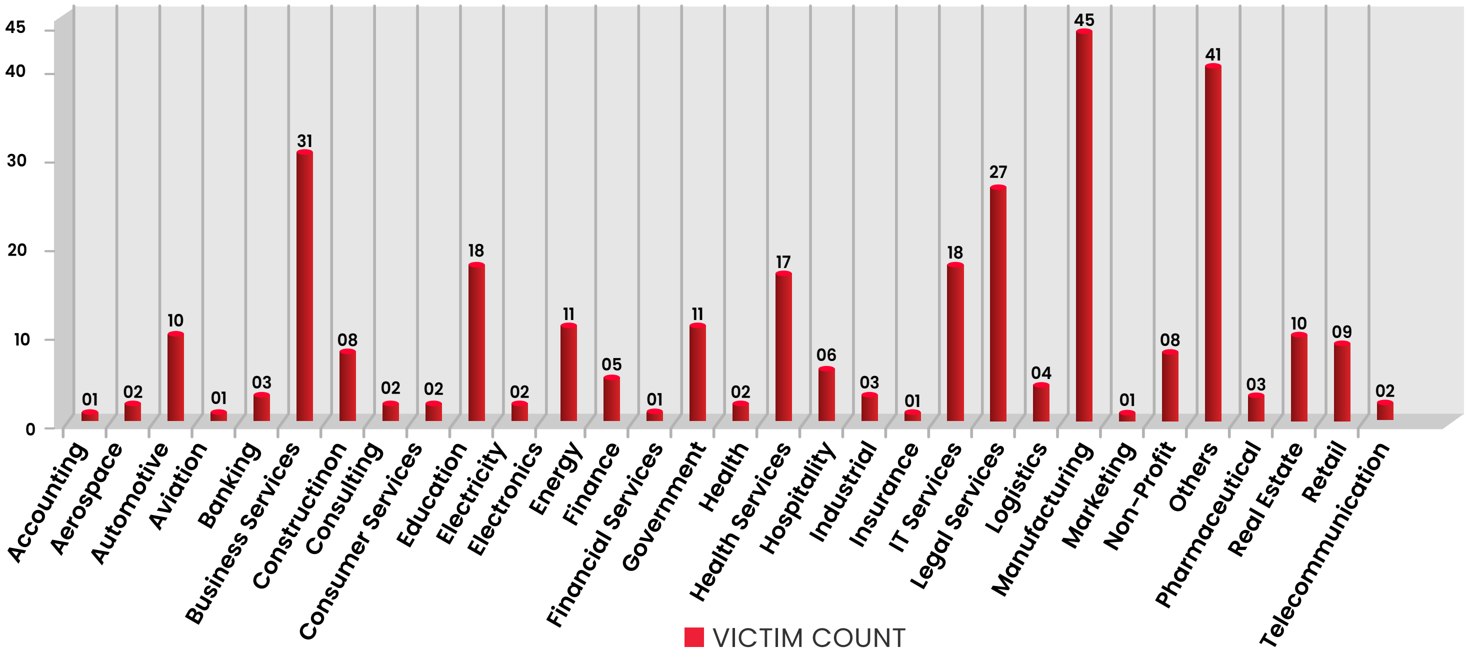
Table of Contents

01

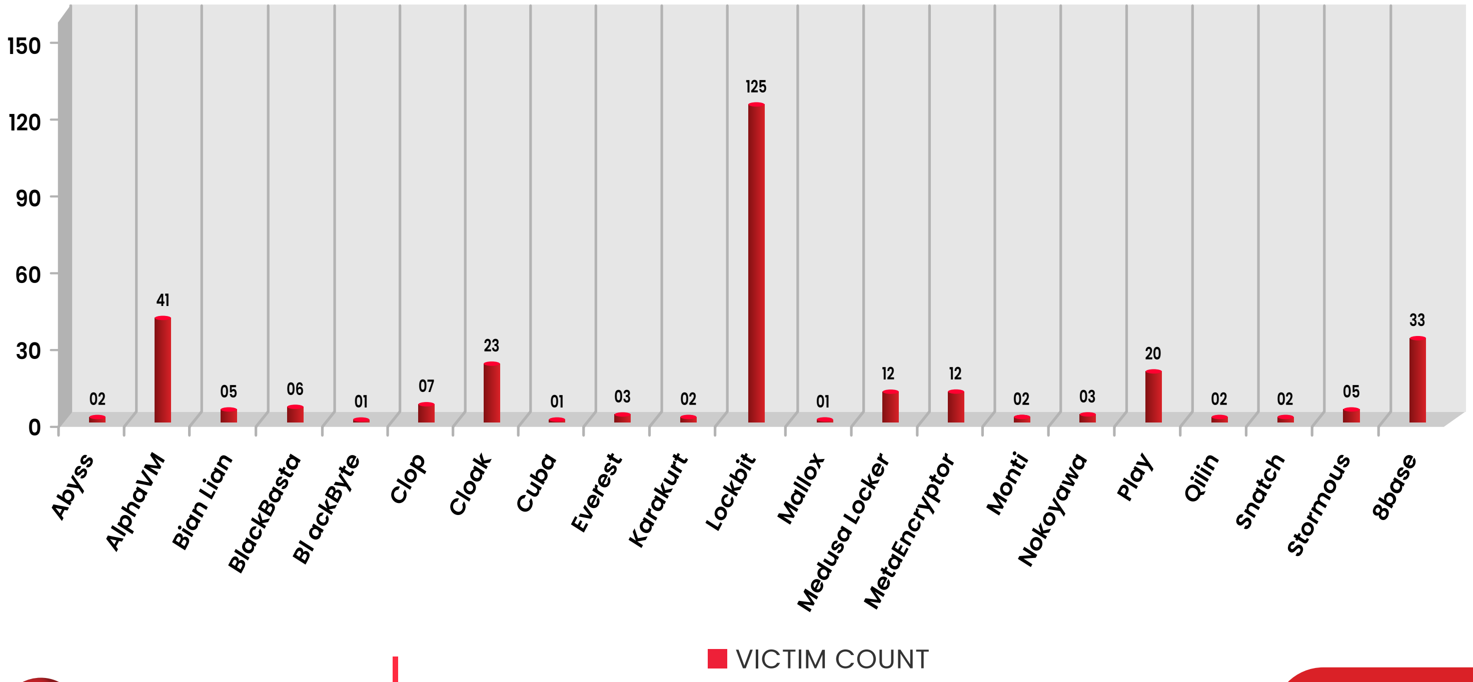
Ransomware Statistics

- Increased attack rate for 8base and BlackCat/AlphVM ransomware.
- Higher number of victims observed from Manufacturing and Business Services, IT and IT services significantly lower.
- Healthcare devices expert Varian claimed to be hacked by Lockbit 3.0 ransomware.
- Fullerton India claimed to be hacked by Snatch ransomware.

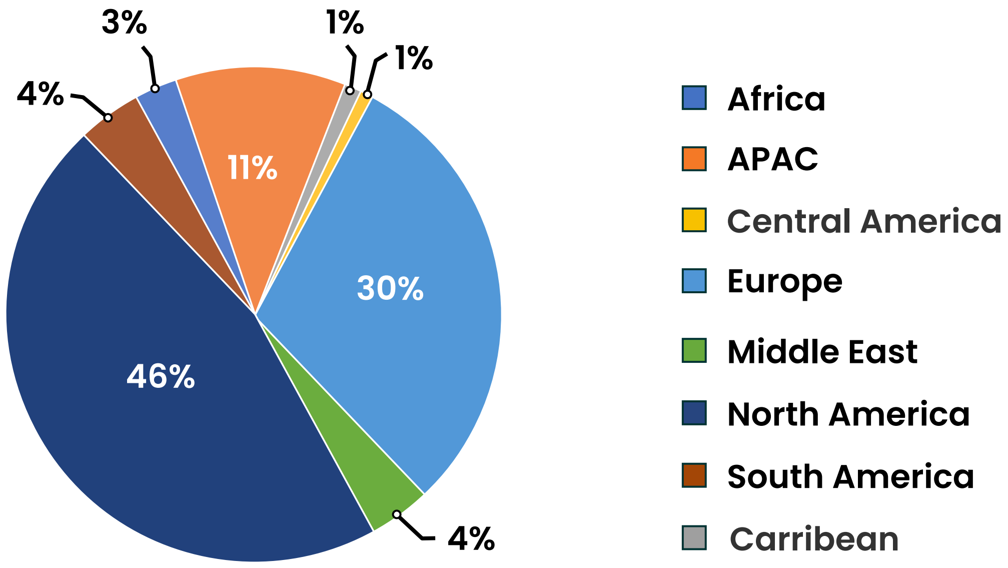
SECTOR-WISE ATTACK TREND



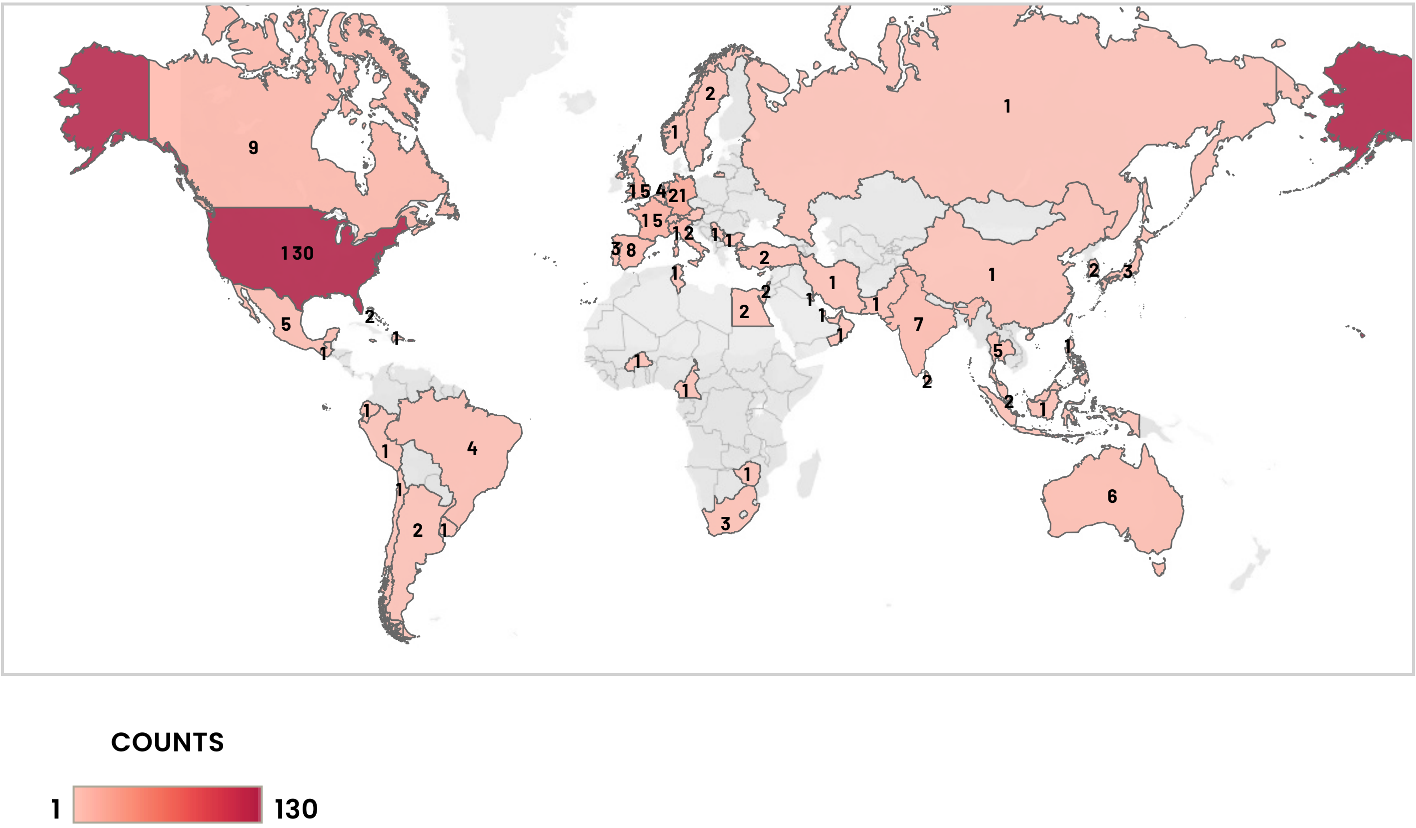
ATTACKS TREND BY RANSOMWARE



REGION-WISE ATTACK



COUNTRY-WISE ATTACK TREND - 308



02

SpyNote Targets Android Devices in Banking Sector

Tags: BFSI, Android, SpyNote malware

In recent years, Cleafy's Threat Intelligence team has been actively investigating Android banking trojans, uncovering techniques like ATO (Automatic Train Operation) and ATS (Automatic Train Supervision) for carrying out bank frauds. However, a concerning shift has emerged in the past months, as the team has observed a surge in spyware infections, with a notable focus on SpyNote malware. Unlike traditional spyware, SpyNote has transitioned to performing bank fraud, marking a disturbing trend in the threat landscape. Other researchers have also reported similar campaigns during this year.

The infection chain of these campaigns often commences with deceptive SMS messages (smishing), prompting users to install a "new certified banking app." Subsequently, victims are directed to a seemingly legitimate app, TeamViewer, known for remote technical support. Disturbingly, attackers are exploiting TeamViewer's functionalities to impersonate bank operators, engaging in fraudulent transactions on victims' devices. Cleafy's analysis reveals that SpyNote, notorious for its wide-ranging capabilities, exploits Accessibility services granted during installation. It does this to facilitate keylogging and automate permission popups. The malware communicates with its command-and-control (C2) server using socket communication, frequently using unusual ports for evasion.

SpyNote employs various defense evasion techniques, including class name obfuscation, junk code insertion, and anti-emulator measures to hinder analysis. Moreover, it dynamically downloads additional files from the C2 server, augmenting its malicious capabilities. This alarming evolution underscores the need for heightened vigilance and security measures against increasingly sophisticated Android banking frauds leveraging spyware like SpyNote.

For IOCs, refer to **Appendix 1A.**

03

Mysterious Bangladesh Launches DDoS Attacks and Data Breaches on India

Tags: India, Mysterious Bangladesh

Hacktivism, a potent cybersecurity threat, often underestimated, poses serious risks to critical infrastructure, telecom, financial, and governmental sectors. Unlike ransomware actors, hacktivists aim to disrupt critical systems, causing severe monetary and reputational damages, without negotiation. Their sophistication rivals financially motivated threat actors, employing malware for large-scale DDoS attacks and data breaches. Collaborative hacktivist groups, exhibiting elevated organization, magnify the danger.

In the Group-IB 2022-23 Hi-Tech Crime Trends report, it's noted that global geopolitical conflicts act as catalysts for hacktivist actions. Mysterious Bangladesh, active since 2020 but prominent since 2022, targets high-level entities across nations, especially India, through over 750 DDoS attacks and 78 website defacements. Their activities extend to web server breaches via known exploits or default credentials.

The report delves into Mysterious Bangladesh's history, attack frequency, targets, affiliations, and motives. Religion and politics drive the group, with the focus on India, evident in four sub-campaigns launched since June 2022. Hacktivists exploit current events for thematic campaigns against specific nations, shifting back to consistent targets like India and Israel. Their strategy centers on countries rather than sectors, often preceded by minor DDoS tests.

Hacktivism, spearheaded by groups like Mysterious Bangladesh, exemplifies the evolving threat landscape, necessitating comprehensive countermeasures to safeguard critical systems and data.

04

Industrial Control Systems Threatened by Critical Vulnerabilities in CODESYS V3

Tags: ICS, OT, CODESYS

Researchers at Microsoft have uncovered multiple high-severity vulnerabilities within the CODESYS V3 software development kit (SDK), a widely used environment for programming programmable logic controllers (PLCs). These vulnerabilities, affecting all CODESYS V3 versions before 3.5.19.0, present a significant risk to operational technology (OT) infrastructure. Potential exploits include remote code execution (RCE) and denial of service (DoS) attacks. This discovery underscores the crucial importance of safeguarding industrial control systems and highlights the need for continuous monitoring and protection of such environments.

With compatibility spanning around 1,000 device types from over 500 manufacturers and millions of devices following the IEC 61131-3 standard, CODESYS is a pivotal tool. A successful DoS attack on a vulnerable CODESYS-powered device could disrupt a power plant, while remote code execution could grant unauthorized access for tampering, abnormal operations, or data theft. Exploiting these vulnerabilities mandates user authentication and in-depth familiarity with CODESYS V3's proprietary protocol and service structure.

Microsoft promptly reported these findings to CODESYS in September 2022, working collaboratively to rectify the vulnerabilities. Security updates have been issued, and users are strongly advised to apply them promptly. This partnership highlights the urgency of addressing such vulnerabilities. CODESYS, a versatile platform-independent solution for automation, empowers developers with tools to implement IEC 61131-3 standards. It includes management software, a simulator for testing, and proprietary protocols utilizing UDP or TCP for communication.

Microsoft researchers demonstrated the exploitation of 12 buffer overflow vulnerabilities for PLC RCE, albeit requiring user authentication and bypassing protective measures like Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR). An additional vulnerability (CVE-2019-9013) facilitated bypassing user authentication by exploiting an unsecured username and password hash, potentially enabling replay attacks. This discovery heightens the need to fortify critical infrastructure against advanced threats, emphasizing the collaborative effort needed to secure industrial control systems against cyber risks.

05

GroupIB's Fraud Matrix Uncovers Gigabud Malware Activities

Tags: Banking Trojan, BFSI, Gigabud

Group-IB's Fraud Matrix, a strategic intelligence tool inspired by the MITRE model, offers a comprehensive analysis of evolving fraudulent techniques across phases. Armed with insights into fraud schemes, operational methods, and recommended defenses, it's a vital resource for organizations to bolster their security posture.

The prime focus of analysis is the Gigabud trojan. Operating through phishing websites in multiple countries, this threat spreads via smishing, urging victims to visit malicious sites for bogus tax refunds. The trojan leverages convincing disguises of government and financial institutions, prompting downloads of malicious Android apps from similar-looking domains.

Android's "Install from Unknown Sources" default setting, a security measure, restricts third-party app installations. However, Gigabud's exploitation of the "REQUEST_INSTALL_PACKAGES" permission, high-risk according to Google, bypasses this barrier. Victims unsuspectingly grant this permission through phishing tactics.

This underscores the need for user vigilance against unusual or suspicious requests. Exploiting legitimate features, Gigabud also captures sensitive information via screen recording. Android's runtime permission offers users control over screen-capturing access.

Gigabud's evolution involves a new keylogging module tailored for banking applications, suggesting its creators are continually refining tactics. The malware's growing adaptability, advanced evasion techniques, and expanding target range highlight the urgency of proactive cybersecurity measures.

06

Monti Ransomware Targets Legal and Government Sectors

Tags: Legal, Government, Monti

The Monti ransomware, notable for its Windows and Linux variants, gained attention due to its striking similarity to Conti ransomware, not just in name but also in tactics. Operating under the alias “Monti,” the group intentionally adopted Conti’s tactics, leveraging their tools and source code. Targeting companies and exposing victims on their leak site, Monti now returns after a two-month hiatus, as per Trend Micro, focusing on legal and government sectors.

A new Linux-based Monti variant, “Ransom.Linux.MONTI.THGOCBC”, diverges its predecessors from predecessors. The variant introduces alterations in command line arguments, incorporating the -whitelist parameter while omitting some older arguments. Tampering with the “/etc/motd” and index.html files, the ransomware replaces their content with a ransom note.

Before encryption, Monti checks file conditions, verifying size and presence of a specific string. It appends an infection marker post-encryption, allowing it to skip files already encrypted based on the marker’s presence. Samples reveal a decryption code, suggesting testing, but it remains ineffective due to lacking the necessary private key.

Organizations are advised to implement robust defense strategies, encompassing data safeguarding protocols, backup procedures, and recovery plans. These measures ensure data security and potential restoration against ransomware attacks, mitigating the impact of encryption or deletion. The resurgence of Monti underscores the continued need for proactive cybersecurity measures across various sectors.

For IOCs, refer to **Appendix 1B.**

07

Phishing Campaigns Use Cloudflare R2 to Evade Detection

Tags: Phishing , Cloudflare

Netskope Threat Labs has uncovered a startling 61-fold surge in traffic to phishing pages hosted on Cloudflare R2. These pages predominantly target Microsoft login credentials, while also aiming at Adobe, Dropbox, and other cloud applications. The attacks are notably directed at victims in North America and Asia, impacting various sectors, including technology, financial services, and banking. Perpetrators exploit Cloudflare R2, a relatively new cloud storage service, for distributing static phishing pages. Evading scrutiny, they employ two key techniques. Cloudflare Turnstile is used to safeguard pages with a CAPTCHA, hindering scanners while permitting victim access. Moreover, many pages deliver malicious content exclusively when referred by another malicious site, ensuring only intended targets receive the phishing content.

Cloudflare R2, introduced in beta in May 2022 and publicly launched in August 2022, offers low-cost static hosting, analogous to Amazon S3 or Google GCS. While offering legitimate services, such platforms often attract malicious use. Within the cloud abuse landscape, R2 is the latest addition, with 167 cloud apps identified for similar malicious content delivery in July. Notably, Cloudflare Turnstile, designed to thwart bots and malicious traffic, features prominently in these attacks. Phishing campaigns leverage it to appear genuine and deter security scanners. Online scanners fail CAPTCHA tests, rendering the actual phishing site inaccessible.

Interestingly, certain phishing pages deploy additional evasion tactics. A timestamp after a hash symbol in the URL triggers the malicious site, while a referring site necessitates a passed parameter. This interdependency conceals the actual phishing page. Both conditions must be met for it to become visible. Furthermore, the phishing site employs Fingerprint BotD, a bot detection library, to identify bot-crawled phishing pages. It responds with custom error codes when bots access the page. As attackers exploit Cloudflare R2 to execute targeted phishing schemes with improved evasion techniques, cybersecurity measures must be enhanced to counter these evolving threats effectively.

08

XLoader targets MacOS through Signed OfficeNote Applications

Tags: Xloader, macOS

XLoader, an enduring malware-as-a-service (MaaS) infostealer and botnet, has resurfaced in a transformed state, shedding dependencies and adopting new evasion tactics. Initially identified in 2015, this malware presented its first macOS variant in 2021, distributed as a Java program. The new version identified by Sentinel One, however, employs C and Objective C languages natively, signing itself with an Apple developer signature and camouflaging as 'OfficeNote', a seeming office productivity app.

Unlike its prior iteration, the new XLoader variant sidesteps Java dependencies and is bundled within a typical Apple disk image named OfficeNote.dmg. The application within bears the developer signature "MAIT JAKHU (54YDV8NU9C)". On execution, the application displays an error message as a cover while surreptitiously installing a persistence agent and depositing the payload, which SentinelOne detects promptly. Upon dropping the payload, XLoader conceals itself in a hidden directory, generating a basic minimal app within, utilizing a copy of itself as the main executable. The malware's persistent behavior persists from previous versions, aiming to pilfer clipboard contents using the Apple API NSPasteboard and generalPasteboard. Chrome and Firefox are targeted browsers, fetching credentials from the "login.json" file in relevant directories. Notably, Safari remains untargeted.

To obfuscate its command-and-control (C2) communications, XLoader employs dummy network calls. The analysis identifies 169 DNS name resolutions and 203 HTTP requests, reaching out to suspicious or malicious IP addresses. The XLoader's renewed tactics highlight its adaptability and ongoing threat to macOS environments. This new XLoader variant poses new challenges to macOS security, emphasizing the necessity for vigilant threat detection and robust cybersecurity measures.

For IOCs, refer to **Appendix 1D.**

09

Lazarus Group Updates Capabilities to Avoid Detections Using New Techniques

Tags: Lazarus, North Korea

Lazarus topic, the North Korean state-sponsored actor, continues to demonstrate its operational confidence by maintaining the use of well-documented infrastructure. This persistence in employing the same tactics, techniques, and procedures (TTPs), many of which are publicly known, underscores the group's audacity and offers avenues for security researchers to counteract their activities. Researchers at Cisco Talos share a detailed report on the same.

In a campaign reported by WithSecure, the group exploited unpatched Zimbra devices and deployed a remote access trojan (RAT) akin to MagicRAT. QuiteRAT, a smaller iteration of MagicRAT, shares capabilities and is based on the Qt framework. The same infrastructure used for QuiteRAT and open-source DeimosC2 agents was previously employed by Lazarus Group for deploying MagicRAT in a campaign from 2022, as well as the newer malware CollectionRAT. Notably, a malicious version of PuTTY's Plink utility was also hosted on this infrastructure, aligning with Lazarus Group's tendency to employ dual-use utilities.

CollectionRAT, signed with a code-signing certificate used for Jupiter/EarlyRAT, encompasses typical RAT capabilities such as command execution and file manipulation. The implant involves a packed Windows binary based on Microsoft Foundation Class (MFC) library, which dynamically decrypts and executes the malware code.

Lazarus Group's approach seems to be evolving. They increasingly use open-source tools and frameworks for initial access rather than just in post-compromise phases. While they once relied on custom-built implants for persistence, they now employ open-source tools like the DeimosC2 framework to establish and maintain initial access. This GoLang-based C2 framework facilitates RAT capabilities, reflecting a shift towards incorporating open-source resources earlier in their attack lifecycle. Lazarus

For IOCs, refer to **Appendix 1E.**

10

SmokeLoader and Whiffy Recon Collect Geolocation Through WiFi Scanning

Tags: SmokeLoader, Whiffy Recon

Secureworks Counter Threat Unit researchers recently uncovered the Smoke Loader botnet deploying a specialized Wi-Fi scanning executable, dubbed "Whiffy Recon," on compromised systems. This malware leverages nearby Wi-Fi access points as data points to triangulate the geographical positions of infected systems, using Google's geolocation API.

Whiffy Recon's operation begins with checking for the presence of the WLANSVC service, indicating wireless capabilities on a Windows system. If detected, the malware creates persistence by generating a wlan.lnk shortcut in the user's Startup folder, linking to the original malware location. The main code encompasses two loops, one registering the bot with the command-and-control (C2) server, and the other conducting Wi-Fi scanning. Upon successful registration, the C2 server responds with a JSON message containing a "secret" UUID, replacing a hard-coded Authorization UUID in future requests. This information is stored in the str-12.bin file. The second loop then initiates Wi-Fi scanning via the Windows WLAN API every 60 seconds.

The scan outcomes are structured in JSON and sent via HTTPS POST to the Google Geolocation API, a legitimate service utilizing Wi-Fi access points and mobile network data to triangulate a system's location. Although the purpose of the geolocation data remains unclear, frequent scanning could facilitate tracking of compromised systems by threat actors. The geolocation information might be exploited for intimidation or coercion purposes, demonstrating the actors' access to this sensitive data.

For IOCs, refer to **Appendix 1F.**

11

Flax Typhoon Uses Legitimate Software to Target Taiwanese Organization

Tags: Flax Typhoon, Taiwan, China

Microsoft has uncovered an espionage campaign orchestrated by the Flax Typhoon (also known as ETHEREAL PANDA) nation-state actor, believed to operate from China. The campaign has predominantly targeted organizations in Taiwan, demonstrating a distinct pattern of malicious activities. While the primary focus remains on Taiwan, the tactics employed are of concern due to their potential for global reusability. Flax Typhoon's motive appears centered on persistent unauthorized access and espionage across diverse industries. Although no definitive objectives have been observed in this campaign, Microsoft has chosen to raise awareness due to the risk it poses to customers and the broader security community.

The campaign involves exploiting known vulnerabilities in public-facing servers, targeting a range of services including VPN, web, Java, and SQL applications. Web shells like China Chopper are used to gain remote code execution on compromised servers. When local administrator privileges are lacking, Flax Typhoon deploys malware like Juicy Potato and BadPotato to elevate privileges. Once inside the system, Flax Typhoon establishes access via RDP, circumventing network-level authentication by altering the Sticky Keys binary. This feature allows the actor to launch the Task Manager with local system privileges when invoking the Sticky Keys shortcut. Further operations involve deploying a VPN connection using SoftEther VPN, downloading it via PowerShell or other LOLBins.

Credential access is a common activity, and the actor also examines restore points, possibly for system comprehension or to remove traces. Since Flax Typhoon relies on valid accounts and LOLBins, detection and mitigation can be challenging. Remedial actions include closing or altering compromised accounts, isolating systems, and implementing mitigation practices. As Flax Typhoon's activity could extend beyond Taiwan, the importance of vigilance and mitigation measures across the security landscape is emphasized.

For IOCs, refer to **Appendix-1G.**

12

Appendix

APPENDIX 1A – SPYNOTE

Hashes
9e185dd6d7137357b61941525e935124
291c24d9b3f4a5793a2600610671eb42

IPs
37.120.141.]144:7771
37.120.141.]140:7775

APPENDIX 1B - MONTI RANSOMWARE

Hashes
f1c0054bc76e8753d4331a881cdf9156dd8b812a
a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef

APPENDIX 1C – CLOUDFLARE TARGETING URLS

URLs
hxxps://pub-de2f439c6744426586c7612824c1bac2.r2[.]dev/index.html?pu=hxxps://pub-7e0ea6c6ac8c439a840ed31912409dc9.r2[.]dev/index.html
hxxp://pub-1f6ee74386dc4dc98c226f8a56f8e8c1.r2[.]dev/office.html
hxxp://pub-9f884b1d186548eea381cab00a0f702c.r2[.]dev/emailverification.html
hxxp://pub-c6542b65e10b483d9136554aa9cb05e8.r2[.]dev/passwordverification.html

hxxp://pub-ca01b8d361b540ce8256226365665de0.r2[.]dev/index2.html
hxxp://pub-a0f9c6938a374a2089f6fad1e6e85d1b.r2[.]dev/index2.html
hxxp://pub-5431347746b0455bb6f7dbc419a23952.r2[.]dev/oeip.html
hxxp://pub-e4b5beda27a847fc9ff07bdb23b36563.r2[.]dev/Dropbox-Business.html
hxxp://pub-7e28a526d64340e89715cafd3ffddee3.r2[.]dev/alocate.html
hxxp://pub-dc7d3a6ae1254ac4b7b0a0873ef10ed1.r2[.]dev/login.html
hxxp://pub-43c8427c1735476fb4e6b1b456757e0a.r2[.]dev/index2.html
hxxp://pub-48d3a24bafe348799aa16e3fbd5ead78.r2[.]dev/001zzz.html
hxxp://pub-5705d571c53847759ca1e27912b57837.r2[.]dev/authr.html
hxxp://pub-b889ecc576cd47b8a7dae94590568f86.r2[.]dev/keep.html
hxxp://pub-d0a002d03d4d4468a1a3a4788d44d971.r2[.]dev/apps.html
hxxp://pub-1abd9bef283343da8c867e32a56a6050.r2[.]dev/link.html
hxxp://pub-4b8c37d5f65746878138f2a1665fc704.r2[.]dev/chi.html
hxxp://pub-9b0c4b61dcdb4349b13b6e0f0902a227.r2[.]dev/OWAOutlook.html
hxxp://pub-16d24eae069c40dcb335224f9555d849.r2[.]dev/diom.html
hxxp://pub-19b440b384f449bc8f30a86a5f3c6049.r2[.]dev/code.html
hxxp://pub-2b0fffc523034ccc9ffa6fb26d5462e5.r2[.]dev/setting.html

hxxp://pub-50137e365ae14a91ad215a40f880bad1.r2[.]dev/link.html
hxxp://pub-6502dddebdc447ed9023277db681dd94.r2[.]dev/vm3.html
hxxp://pub-d3ef7b90634c41c2aea65d57a1da514f.r2[.]dev/dashworkers.html
hxxp://pub-d1729d90c762460c9395a066038cdaf9.r2[.]dev/background-full.html
hxxp://pub-51b3ca6392244b5bb14982b7ddf92f27.r2[.]dev/gaames.html
hxxp://pub-c27949832b64423ab5f75bafdf57ba92.r2[.]dev/authe.html
hxxp://pub-00268bd240fc441cb2f8557a6961d87d.r2[.]dev/verywebmail.html
hxxp://pub-b2955bd5cc5a447cba7f9017e8915538.r2[.]dev/webmail.html
hxxp://pub-93bd771473c24746860b98ace628fe91.r2[.]dev/ourteam.html
hxxp://pub-28dfeb6275f8415ba3e6b97dfff9ccfc.r2[.]dev/0012823733.html
hxxp://pub-9008e63dbf464532acb4ebdafa3bfb86.r2[.]dev/S3M6S5.html
hxxp://pub-1b0adb2146a640a0b0ec2645f84b6a9a.r2[.]dev/shaaa.html
hxxp://pub-7c6128fbcd6a4ed3a12554f7446ffe16.r2[.]dev/inslo.htm
hxxp://pub-4054e7f05a57459e88c44b940037f4fb.r2[.]dev/wnnslo.htm
hxxp://pub-1df03b95474e44baa86a0a11a33527d0.r2[.]dev/welcome.html
hxxp://pub-5d09e89ff38240f2b559297a9206beea.r2[.]dev/auth.html
hxxp://pub-9064d4445dc3440599c3d2cab66301d9.r2[.]dev/verication.html

hxxp://pub-a8f7a7bdbbef4c7aa377b495dabb19ff.r2[.]dev/saved.html
hxxp://pub-c8dc8d57c6e24653a737a5acb81893ee.r2[.]dev/office365.html
hxxp://pub-b0879d66c06e4547a6fe4d002fc9f88e.r2[.]dev/xtrst.html
hxxp://pub-c92a4cf1fb774dd79b9c7d32023ab3fa.r2[.]dev/llo.html
hxxp://pub-1cd83eaf4a66425d86fb1e8f37610be0.r2[.]dev/index.html
hxxp://pub-7e71a0ecd46d4dc0ac25e43cbb595918.r2[.]dev/index.html
hxxp://pub-44c085b5c63b4a438aed0cd194363508.r2[.]dev/index2.html
hxxp://pub-f488d77bc04a4676ad79ee159fe7d8c5.r2[.]dev/index2.html
hxxp://pub-3b2c4103dbe84e8081aa257826f25d54.r2[.]dev/noon.html
hxxp://pub-62c47a7a8e0a4ca293b31ee18b2baf43.r2[.]dev/EmailVerification.html
hxxp://pub-887adfef303443cc97eee0e66e6d6dbc.r2[.]dev/nick.html
hxxp://pub-fbf017af618541b3a76abd75f8dab1b7.r2[.]dev/new.html
hxxp://pub-ecff9b63c2c1497bbcbe5d573900b143.r2[.]dev/oml.html
hxxp://pub-0e459479bb894ae6a3446ba7783965b0.r2[.]dev/docusign encrypted.htm
hxxp://pub-3a226c66bcda41e4bbeec4790c71c89c.r2[.]dev/lanx_sl1.htm
hxxp://pub-5c8b0c206b484f208b18e2c09e806156.r2[.]dev/HX-ADFS_9.html
hxxp://pub-cc4afac7b0304f62946883c1b996ddc3.r2[.]dev/bookingmail.html

hxxp://pub-5c0aa65f5f224858a03e429b595c1811.r2[.]dev/dropbox-sign-in.html
hxxp://pub-422f33674c4b4fe182123a25dbb97378.r2[.]dev/secu3.html
hxxp://pub-b2955bd5cc5a447cba7f9017e8915538.r2[.]dev/micr@s0ft.html
hxxp://pub-62d1a4086e2a4406ae5e1a788e7a019b.r2[.]dev/action.html
hxxp://pub-dda005a462634fea953ace187610f4c7.r2[.]dev/nexc.html
hxxp://pub-54efd4aa11884bfb834031d41082f502.r2[.]dev/res.html
hxxp://pub-45f4523b469c4ea18afe1c70ebaabeda.r2[.]dev/index.html
hxxp://pub-9eaf08966d54441789d558bfe758e12c.r2[.]dev/Diceyencode.html
hxxp://pub-b08c2d9bbe594efba55b1b8d4009a382.r2[.]dev/sam365.html
hxxp://pub-99eed73366de4872bbe331bbbfb758cf.r2[.]dev/email.html

APPENDIX 1D- XLOADER

Hashes
26fd638334c9c1bd111c528745c10d00aa77249d
47cacf7497c92aab6cded8e59d2104215d8fab86
5946452d1537cf2a0e28c77fa278554ce631223c
958147ab54ee433ac57809b0e8fd94f811d523ba

IPs
23[.]227.38[.]74
62[.]72.14[.]220
66[.]29.151[.]121
104[.]21.26[.]182
104[.]21.32[.]235
104[.]21.34[.]62
137[.]220.225[.]17
142[.]251.163[.]121

URLs
www[.]activ-ketodietakjsy620[.]cloud
www[.]akrsnamchi[.]com
www[.]brioche-amsterdam[.]com
www[.]corkagenexus[.]com
www[.]growind[.]info
www[.]hatch[.]computer
www[.]kiavisa[.]com
www[.]lushespets[.]com
www[.]mommachic[.]com
www[.]nationalrecoveryllc[.]com
www[.]pinksugarpopmontana[.]com
www[.]qhsbobfv[.]top
www[.]qq9122[.]com
www[.]raveready[.]shop

www[.]spv88[.]online
www[.]switchmerge[.]com

APPENDIX 1E – LAZARUS GROUP

Hashes
ed8ec7a8dd089019cfd29143f008fa0951c56a35d73b2e1b274315152d0c0ee6
db6a9934570fa98a93a979e7e0e218e0c9710e5a787b18c6948f2eedd9338984
773760fd71d52457ba53a314f15dddb1a74e8b2f5a90e5e150dea48a21aa76df

IPs
146[.]4[.]21[.]94
109[.]248[.]150[.]13
108[.]61[.]186[.]55:443

URLs
hxxp[://]146[.]4[.]21[.]94/tmp/tmp/comp[.]dat
hxxp[://]146[.]4[.]21[.]94/tmp/tmp/log[.]php
hxxp[://]146[.]4[.]21[.]94/tmp/tmp/logs[.]php
hxxp[://]ec2-15-207-207-64[.]ap-south-1[.]compute[.]amazonaws[.]com/resource/main/rawmail[.]php
hxxp[://]109[.]248[.]150[.]13/EsaFin[.]exe
hxxp[://]146[.]4[.]21[.]94/boards/boardindex[.]php
hxxp[://]146[.]4[.]21[.]94/editor/common/cmod

APPENDIX 1F – SMOKELOADER AND WHIFFY RECON

Hashes
009230972491f5f5079e8e86e19d5458
8532e67e1fd8441dc8ef41f5e75ee35b0d12a087
935b44784c055a897038b2cb6f492747c0a1487f0ee3d3a39319962317cd4087

Network Indicators
194[.]87[.]32[.]20
hxxp://195[.]123[.]212[.]53/wlan.exe

APPENDIX 1G – FLAX TYPHOON

IPs
101.33.205[.]106
39.98.208[.]61
45.195.149[.]224
122.10.89[.]230
45.204.1[.]248
45.204.1[.]247
45.88.192[.]118
154.19.187[.]92
134.122.188[.]20
104.238.149[.]146

139.180.158[.]51
192.253.235[.]107

Hashes
7992c0a816246b287d991c4ecf68f2d32e4bca18
5437d0195c31bf7cedc9d90b8cb0074272bc55df
cc1f0cdc131dfafd43f60ff0e6a6089cd03e92f1
2c95b971aa47dc4d94a3c52db74a3de11d9ba658

Payatu's Security Capabilities

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

CTI

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting – Strategic, Operational and Tactical Intelligence, Risk Monitoring through social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platforming monitoring done for their brand.

Web Security Testing

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

Product Security

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components "fit" together in your mega-product.

Mobile Security Testing

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.

Cloud Security Assessment

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared. As long as cloud servers live on, the need to protect them will not diminish.

Both cloud providers and users have a shared responsibility to secure the information stored in their cloud Payatu's expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.

Code Review

Payatu's Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.

Red Team Assessment

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization's crown jewels and test its readiness to detect and withstand a targeted attack.

DevSecOps Consulting

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.

Critical Infrastructure Assessment

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation Systems, etc., that can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your critical infrastructure.

IoT Security Testing

IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.