Payatu

September 2023

Cyber Threat Intelligence Report

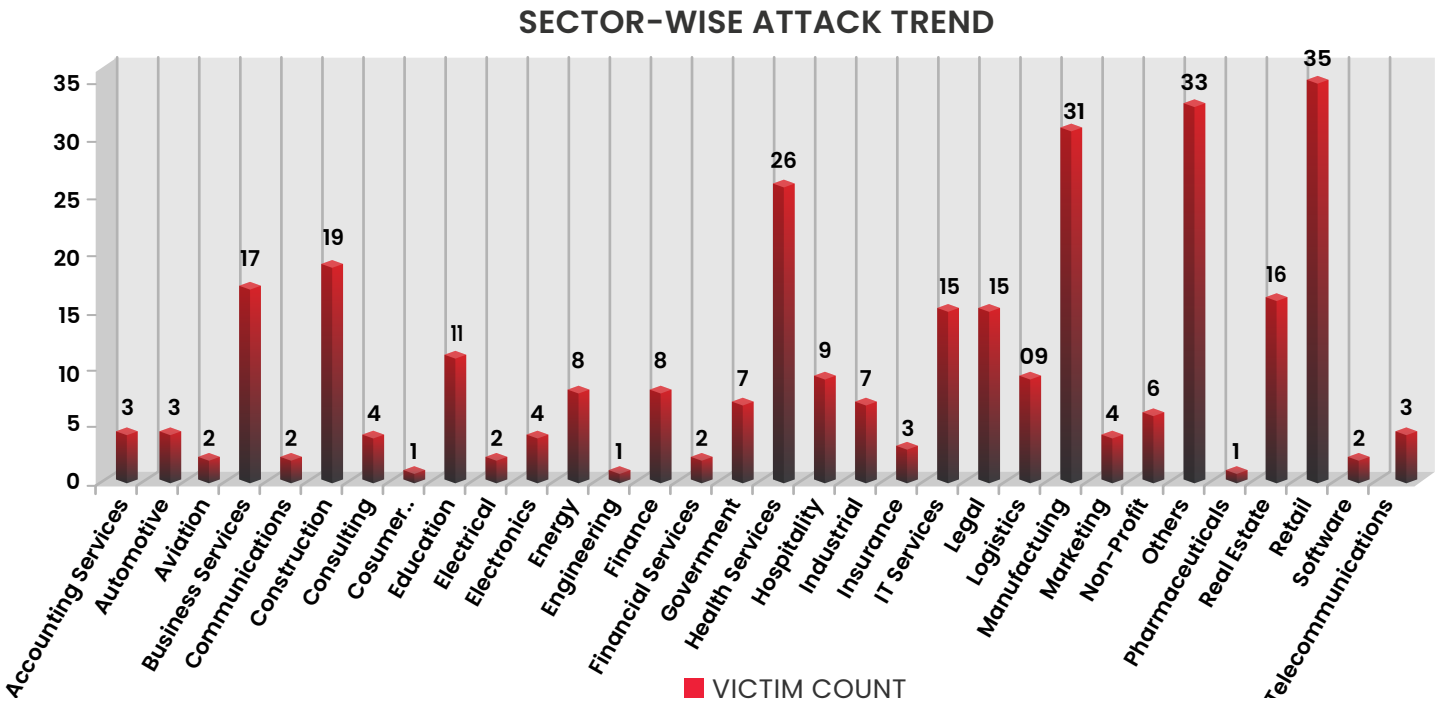
Payatu Security Consulting Pvt. Ltd.

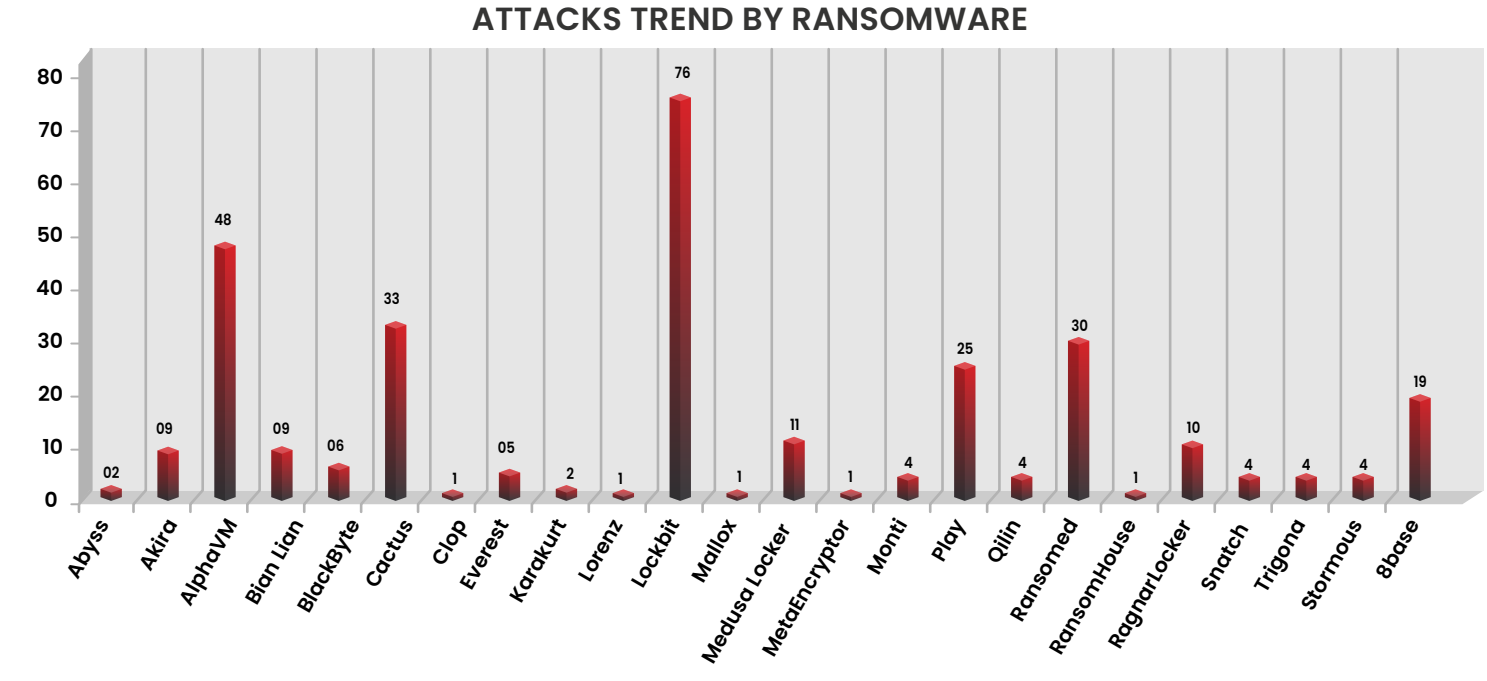
Table of Contents

01

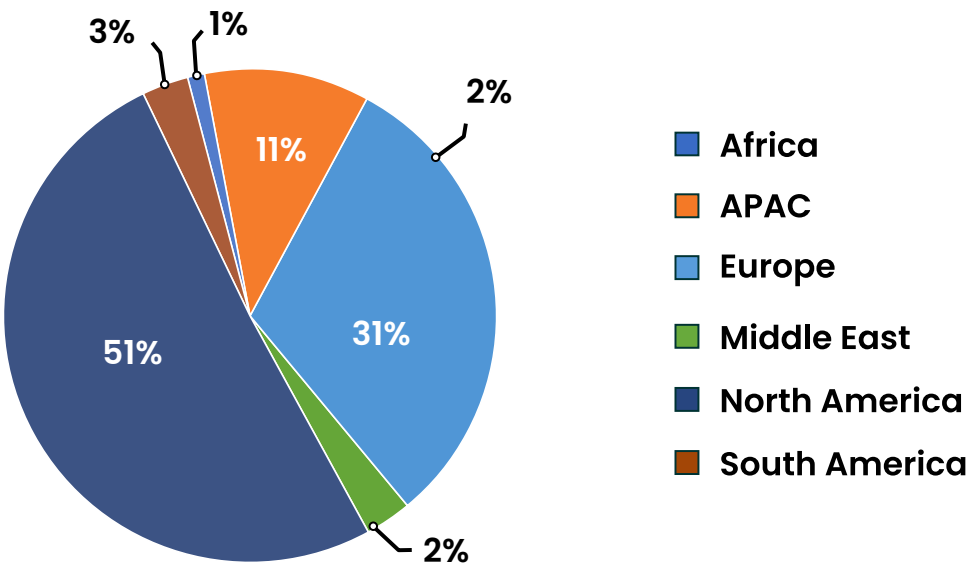
Ransomware Statistics

- MGM Resorts International climed to be compromised by AlphVM/Blackcat ransomware.
- Epson, the Electronic giant compromised by Stormous ransomware.
- American Healthcare giant, Prestige Care compromised by AlphVM/Blackcat ransomware.
- Motel One, a low budget hotel chain from Germany compromised, Blackcate leaks data over its site.
- Sony Group confirms to be compromised by Clop ransomware.

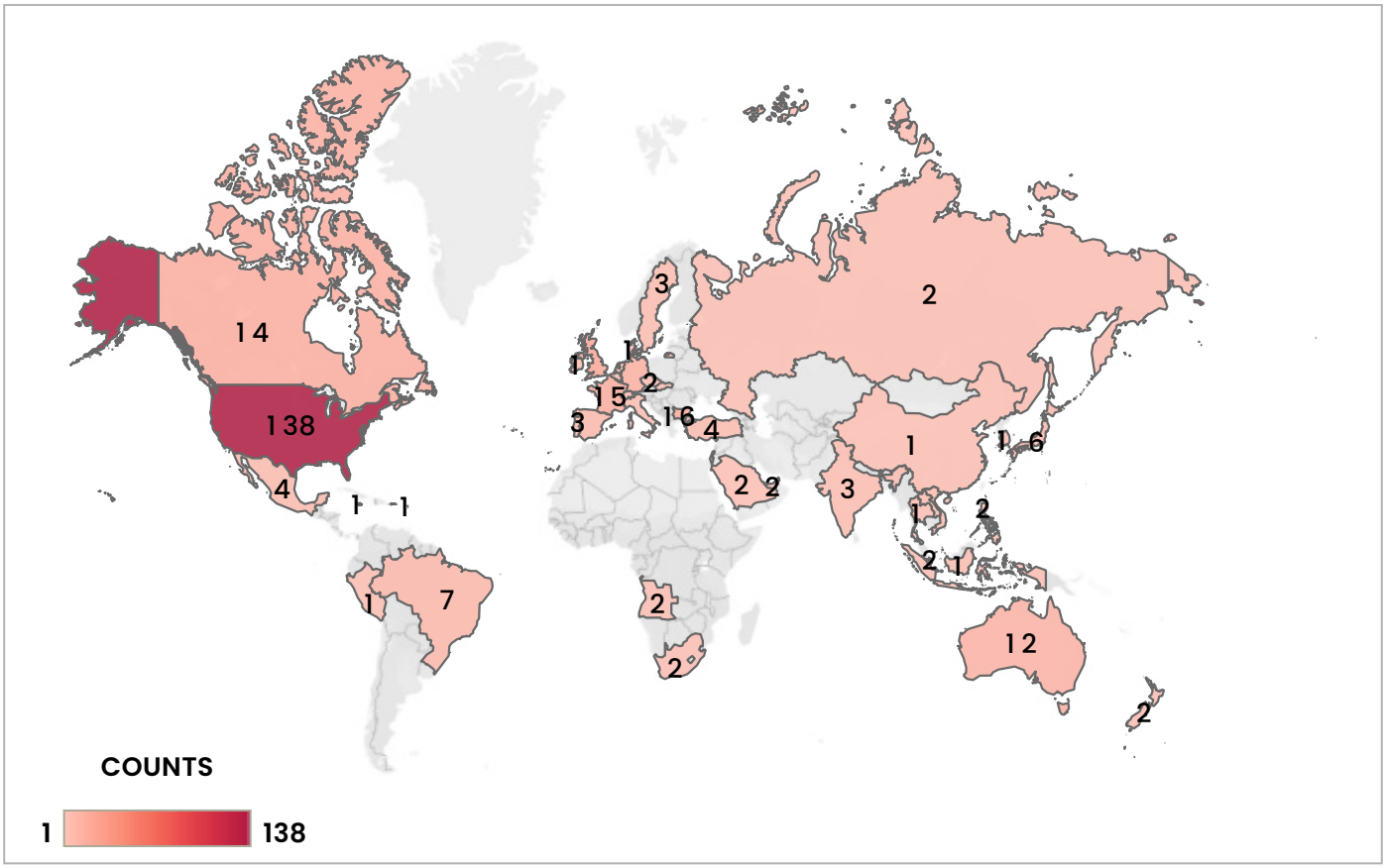




REGION-WISE ATTACK



COUNTRY-WISE ATTACK TREND - 310



02

The Elusive Tactics of ShadowSyndicate: A Deep Dive into its Activities

Tags: Ransomware, RaaS

ShadowSyndicate, distinct from Shadow ransomware, has been raising eyebrows in the cybersecurity realm with its uncommon practices. The threat actor identified by Group-IB utilizes a singular Secure Shell (SSH) fingerprint across an astounding 85 servers, an unusual occurrence given that each SSH fingerprint typically identifies a unique server host key. Since its emergence in July 2022, the group has demonstrated considerable versatility, employing seven distinct ransomware families within a year. Their affiliation remains uncertain, but evidence suggests they are a RaaS (Ransomware as a Service) partner. ShadowSyndicate's comprehensive toolkit comprises off-the-shelf tools like Cobalt Strike, IcedID, and Sliver malware. A significant 52 of their servers functioned as Cobalt Strike C2 frameworks. Their activities can be confidently linked to Quantum, Nokoyawa, and ALPHV ransomware campaigns. Tentative links also suggest involvement with Royal, Cl0p, Cactus, and Play ransomware operations. An intriguing connection was discovered between ShadowSyndicate's infrastructure and Cl0p/Truebot.

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

03

The Resurgence of Xenomorph Malware

Tags: Xenomorph, Spain, Canada, Mobile banking trojan

In February 2022, the Xenomorph malware surfaced, showing eerie resemblances to its film counterpart. By August 2023, ThreatFabric discovered new samples, showcasing evolved tactics like phishing webpages to trick users into harmful APK downloads. The updated version targets numerous US and Portuguese institutions and crypto wallets, reflecting a broader malware trend. Dominant in Spain and the US, its campaign heavily focuses on devices from market leaders, Samsung and Xiaomi. Xenomorph's modus operandi involves overlays to extract user data, and while its technical core remains stable, new features like "antisleep" and "mimic" enhance its potency. It is distributed primarily through phishing pages masquerading as Chrome updates. This surge in activity underscores the continuous evolution of cyber threats, with Xenomorph diversifying its targets and refining its techniques.

04

Espionage Attacks on Southeast Asia

Tags: Southeast Asia, Chinese threat actors

In 2023, Unit 42 researchers embarked on an investigation into espionage attacks aimed at a Southeast Asian government. These cyber-espionage efforts targeted a myriad of governmental sectors, from public healthcare to critical infrastructure. Originally, it was assumed that a singular threat actor orchestrated these attacks. However, meticulous scrutiny unveiled the involvement of three separate threat entities, each showcasing unique modus operandi.

The first cluster, CL-STA-0044, was confidently attributed to the Stately Taurus group, also known as Mustang Panda, which is widely believed to be linked to Chinese interests. The second, CL-STA-0045, was tied to the Alloy Taurus group, another faction suspected of operating on behalf of the Chinese state. The third, CL-STA-0046, was connected to the Gelsemium group, but its affiliations to any specific state remain undetermined.

Spanning activities from 2021 and onwards, these revelations underscore the persistent and evolving nature of Advanced Persistent Threats (APTs). Utilizing the Diamond model of attribution, this research emphasizes the complexities involved in discerning discrete cyber threats, underscoring the imperative of maintaining vigilance against these adept adversaries in an ever-evolving digital landscape.

05

Sandman, a New Threat Actor Targeting Middle East

Tags: Sandman, Lua, Middle East, Asia

SentinelLabs uncovered a novel threat in 2023, naming the actor Sandman. This unidentified entity primarily targets telecommunication providers across the Middle East, Western Europe, and South Asia. Characterized by strategic movements and minimal engagements, Sandman's operations suggest stealth objectives. The actor introduced a unique modular backdoor, LuaDream, exploiting the LuaJIT platform, hinting at a well-structured, extensive project.

While LuaDream's origin remains nebulous, its operational style and the disparity between high-quality development and poor segmentation suggest the work of private contractors, similar to groups like Metador. SentinelLabs' August observations highlighted Sandman's targeted attacks on the telecom sector, using the meticulously designed LuaDream to evade detection.

Sandman's operations involve credential theft, reconnaissance, and targeted workstation infiltrations, specifically targeting managerial roles. Although Sandman's roots remain undetermined, its operations and tools, especially LuaDream, exemplify the cyber espionage world's continuous innovation.

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

06

Microsoft's Accidental Data Exposure

Tags: Microsoft, Data leak

Microsoft's AI research team mistakenly exposed 38 terabytes of private data on GitHub, including a disk backup from two employees, secrets, private keys, passwords, and over 30,000 Microsoft Teams messages. The error occurred while using Azure's SAS tokens. Intended to share specific files, a misconfiguration shared the entire storage account instead.

This incident sheds light on the challenges faced when harnessing AI. As engineers handle massive AI training data, the demand for robust security becomes paramount. Exacerbating this misstep, the token not only granted excessive access but also enabled "full control," allowing potential attackers to overwrite or delete files.

The repository was designed to provide AI models for code training. Yet, the .ckpt file format used, tied to TensorFlow and Python's pickle formatter, is inherently vulnerable to arbitrary code execution. This vulnerability could have let attackers compromise the AI models, posing risks to any user accessing Microsoft's GitHub repository. This situation emphasizes the urgency for stringent data security and meticulous configurations in AI advancements.

07

3AM Ransomware: A New Contender in the Cyber Threat Landscape

Tags: 3AM ransomware

A novel ransomware named 3AM has recently been identified, with its usage so far being quite limited. Symantec's Threat Hunter Team, a segment of Broadcom, witnessed it being employed in one attack. Initially, the ransomware affiliate tried deploying LockBit on the target's network. However, when that attempt was thwarted, the affiliate pivoted to using 3AM.

3AM, crafted in Rust, is believed to be a fresh malware family. The modus operandi involves terminating various services on the infected machine before initiating file encryption. Post encryption, it seeks to erase Volume Shadow (VSS) copies, eliminating potential recovery options for the victim. Whether the developers of 3AM have affiliations with recognized cybercriminal groups remains uncertain.

Upon execution, 3AM scans the disk, encrypting files that match certain criteria, subsequently deleting the originals. Each affected folder gets a "RECOVER-FILES.txt" file, which serves as the ransom demand note. A unique marker string "0x666" is appended to the encrypted files.

It's noteworthy that ransomware affiliates are exhibiting increasing autonomy from their parent ransomware entities. Symantec's encounter with an affiliate deploying two distinct ransomware in a single attack isn't unprecedented.

While new ransomware families frequently emerge and often fade swiftly, 3AM's selection as a LockBit backup could signify its potential appeal to cyber attackers, suggesting that we might encounter it again.

For Appendix, refer to **Appendix - 1C.**

08

Microsoft Identifies New Storm-0324 Phishing Campaigns

Tags: Storm-0324, Microsoft

Microsoft has been tracking Storm-0324, a finance-oriented threat actor that typically commences attacks with email-based phishing methods. They then hand off the compromised network access to secondary threat actors, often resulting in ransomware attacks. By July 2023, Storm-0324 adopted a new tactic: using an open-source tool to dispatch phishing lures via Microsoft Teams chats. This move is distinct from the Midnight Blizzard campaigns on Teams from May 2023. Early interception and remediation of Storm-0324 can avert severe subsequent threats like ransomware.

Known to other researchers as TA543 and Sagrid, Storm-0324 operates as a distributor in the cybercrime sphere. Its speciality lies in dispersing other attackers' payloads through phishing and exploit kits. Its modus operandi revolves around evasive infection chains with payment and invoice-based lures. It distributes JSSLoader malware, enabling access for the ransomware-as-a-service actor, Sangria Tempest. Historically, its distributions have included the Gozi infostealer and Nymaim downloader and locker.

Storm-0324's email campaigns often imitate services like DocuSign and Quickbooks, directing users to a SharePoint-hosted zipped file, which contains JavaScript to download the malicious payload. It has deployed multiple file formats to release the malicious JavaScript, including Microsoft Office documents and Windows Script File (WSF).

By July 2023, Storm-0324 innovated further by sending phishing lures through Teams containing malicious links to SharePoint-hosted files. This tactic likely employs a tool named TeamsPhisher, allowing users to attach files in Teams messages sent externally. This can be manipulated by attackers to send phishing attachments, with such lures tagged as "EXTERNAL" users by Teams if the organization permits external access.

09

Sony Hacked, Data up for Sale on Darkweb

Tags: Sony, Ransomware

Sony is currently investigating allegations of a recent cyberattack, with multiple hacking entities claiming responsibility, as shared by Bleeping Computer. Initially, RansomedVC, an extortion group, proclaimed they had breached SONY[.]com and aimed to sell its "data and access". They showcased a minuscule sample on their leak site, even though they claimed to have extracted 260 GB of Sony's data, setting a price tag of $2.5 million. In contradiction to their title, RansomedVC indicated that they are more of an extortion group rather than a dedicated ransomware entity. In response, a Sony spokesperson verified the ongoing investigations but did not offer detailed comments.

Adding to the complexity, another cyber actor named 'MajorNelson' has also staked a claim on the Sony attack. 'MajorNelson' criticized the media for hastily believing RansomedVC and labeled them as scammers seeking attention. They also listed the contents of their alleged breach, covering various credentials and Sony's internal policies. As the situation unfolds, discerning the real attacker becomes increasingly challenging.

10

BunnyLoader, a new Malware-as-a-Service on Sale

Tags: MaaS

In September, Zscaler ThreatLabz identified a fresh Malware-as-a-Service (MaaS) threat named "BunnyLoader" available for purchase on multiple forums. This malicious software offers a variety of features, including downloading secondary payloads, pilfering browser credentials, system data, and more. Notably, it uses a keylogger to capture keystrokes and a clipper that replaces genuine cryptocurrency wallet addresses on a victim's clipboard with ones controlled by the cyber attackers. BunnyLoader subsequently packs the gathered data into a ZIP file and forwards it to its command-and-control (C2) server.

From its inception on September 4, 2023, BunnyLoader has seen brisk development. Within just 25 days, multiple feature updates and bug resolutions have been rolled out. This has included amendments to its C2 panel, bug resolutions, and even revamped pricing structures. The C2 panel of BunnyLoader lists diverse functionalities, such as keylogging, credential theft, clipboard manipulation for cryptocurrency theft, remote command execution, and more. Given its rapid evolution and expanding capabilities, BunnyLoader poses a significant MaaS threat.

11

Appendix

APPENDIX 1A – SHADOW SYNDICATE

IP Addresses
109.172.45[.]28
109.172.45[.]77
141.98.82[.]201
146.70.116[.]20
147.78.47[.]219
147.78.47[.]231
147.78.47[.]235
147.78.47[.]241
158.255.2[.]244
158.255.2[.]245
158.255.2[.]252
179.60.146[.]10
179.60.146[.]11
179.60.146[.]25
179.60.146[.]5
179.60.146[.]51
179.60.146[.]52
179.60.146[.]6
179.60.150[.]117
179.60.150[.]121
179.60.150[.]125
179.60.150[.]132
179.60.150[.]139
179.60.150[.]151
193.142.30[.]154
193.142.30[.]17

193.142.30[.]205
193.142.30[.]215
193.29.13[.]148
193.29.13[.]202
194.135.24[.]241
194.135.24[.]244
194.135.24[.]246
194.135.24[.]247
194.135.24[.]248
194.135.24[.]253
194.135.24[.]254
194.165.16[.]53
194.165.16[.]60
194.165.16[.]62
194.165.16[.]63
194.165.16[.]64
194.165.16[.]83
194.165.16[.]90
194.165.16[.]91
194.165.16[.]92
194.165.16[.]99
212.113.106[.]118
212.224.88[.]71
45.182.189[.]105
45.182.189[.]106
45.182.189[.]110
45.227.252[.]247
45.227.252[.]252
45.227.253[.]20
45.227.253[.]29
45.227.253[.]30
45.227.255[.]189

45.227.255[.]214
46.161.27[.]133
46.161.27[.]151
46.161.27[.]160
46.161.40[.]164
5.188.86[.]206
5.188.86[.]227
5.188.86[.]234
5.188.86[.]235
5.188.86[.]236
5.188.87[.]47
5.8.18[.]117
5.8.18[.]242
5.8.18[.]245
78.128.112[.]139
78.128.112[.]207
79.137.202[.]45
81.19.135[.]249
81.19.136[.]239
81.19.136[.]241
81.19.136[.]249
81.19.136[.]250
81.19.136[.]251
88.214.26[.]38
91.238.181[.]240
91.238.181[.]247
81.19.135[.]229
193.142.30[.]211
45.227.252[.]229
193.142.30[.]37
78.128.112[.]220
5.188.87[.]54
5.188.87[.]41

Hashes
aerosunelectric[.]com
asaper[.]xyz
asapor[.]xyz
asaporeg[.]xyz
aserpo[.]xyz
assapaa[.]xyz
avdev[.]net
cache01.micnosoftupdate[.]com
cmdatabase[.]com
d4ng3r.s01kaspersky[.]com
devcloudpro[.]com
devsetgroup[.]com
dsvchost[.]com
eastzonentp[.]com
esoftwareupdates[.]com
expotechsupport[.]com
herbswallow[.]com
ipulsecloud[.]com
maximumservers[.]net
msupd.wimdowupdate[.]com
mysqlserver[.]org
opentechcorp[.]net

paloaltocloud[.]online
powersupportplan[.]com
qw.sortx2[.]com
qw.sveexec[.]com
qw.vm3dservice[.]com
settingdata[.]com
situotech[.]com
upd232.windowservicecentar[.]com
uranustechsolution[.]com
webtoolsmedia[.]com
windosupdate[.]net
etgtgvtgttefeer[.]xyz
egetrgertgegege[.]xyz
egetrgertgeb[.]xyz
egetrgertgebrtgf[.]xyz
egetrgertgegegevgvyub[.]xyz
svchostsreg[.]com

APPENDIX 1B - MONTI RANSOMWARE

SHA-1
1cd0a3dd6354a3d4a29226f5580f8a51ec3837d4
27894955aaf082a606337ebe29d263263be52154
5302c39764922f17e4bc14f589fa45408f8a5089
77e00e3067f23df10196412f231e80cec41c5253

b9ea189e2420a29978e4dc73d8d2fd801f6a0db2
fb1c6a23e8e0693194a365619b388b09155c2183
ff2802cdbc40d2ef3585357b7e6947d42b875884

C2 domains
mode.encagil[.]com
ssl.explorecell[.]com

APPENDIX 1C – 3AM RANSOMWARE

SHA-256
079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22
307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e
680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4
991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af
ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc

C2 domains
185.202.0[.]111
212.18.104[.]6
85.159.229[.]62

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.