Payatu

July 2023

Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

Table of Contents

A.
Ransomware Statistics 03

B.
Rising Threat of Mallox Ransomware, Expanded Activities 05

C.
APT41 Exploits Android Mobile Phones via WyrmSpy and DragonEgg 06

D.
FIN8 Group Exploits POS Devices Using Noberus Ransomware and Sardonic Backdoor 07

E.
Use of AI by Threat Actors Simplified by WormGPT and FraudGPT 08

F.
Microsoft Thwarts Storm-0558's Attack on Azure AD and Outlook Infrastructure 09

G.
Critical Vulnerabilities Identified in Rockwell Automations ControlLogix Systems 10

H.
A Mexican Threat Actor - Neo_Net targeting Global Banks in Recent Campaign 11

I.
Rustbucket Targets MacOS Users 12

K.
VirusTotal Data Leak Exposes Security Researchers 12

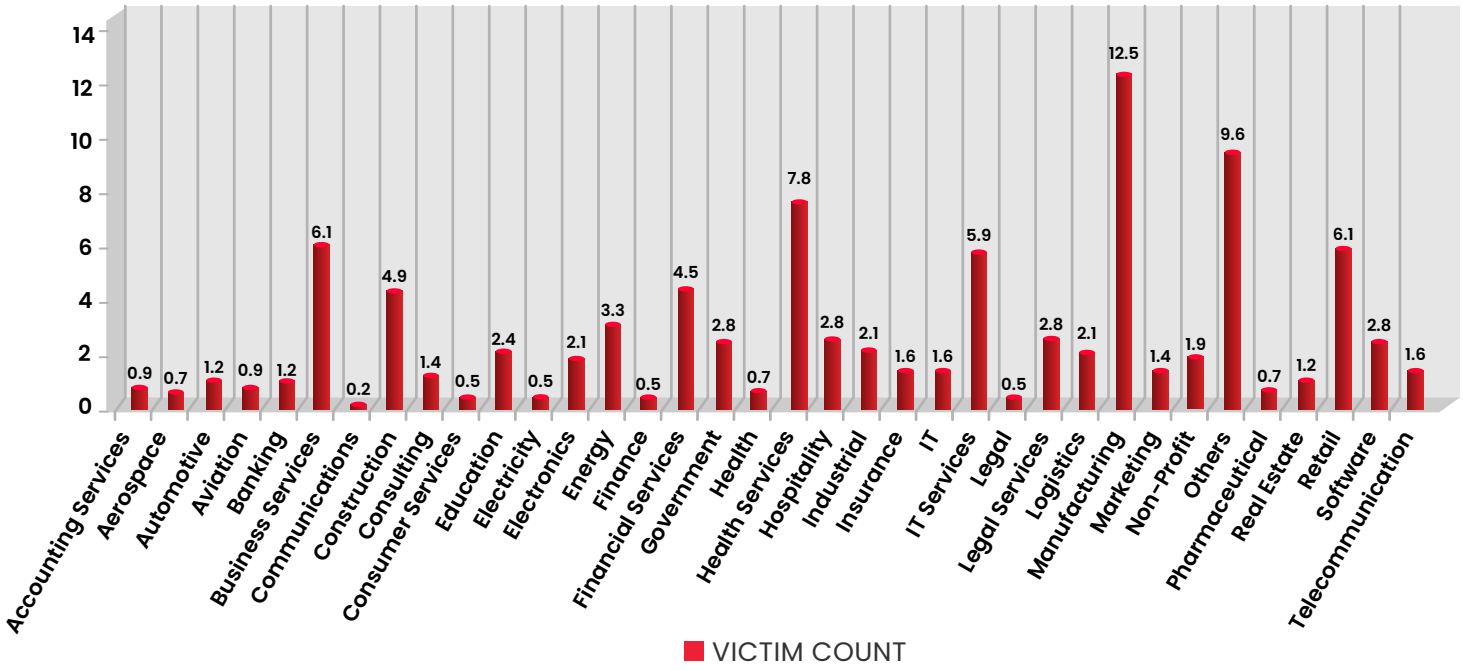
K.
Appendix 14

01

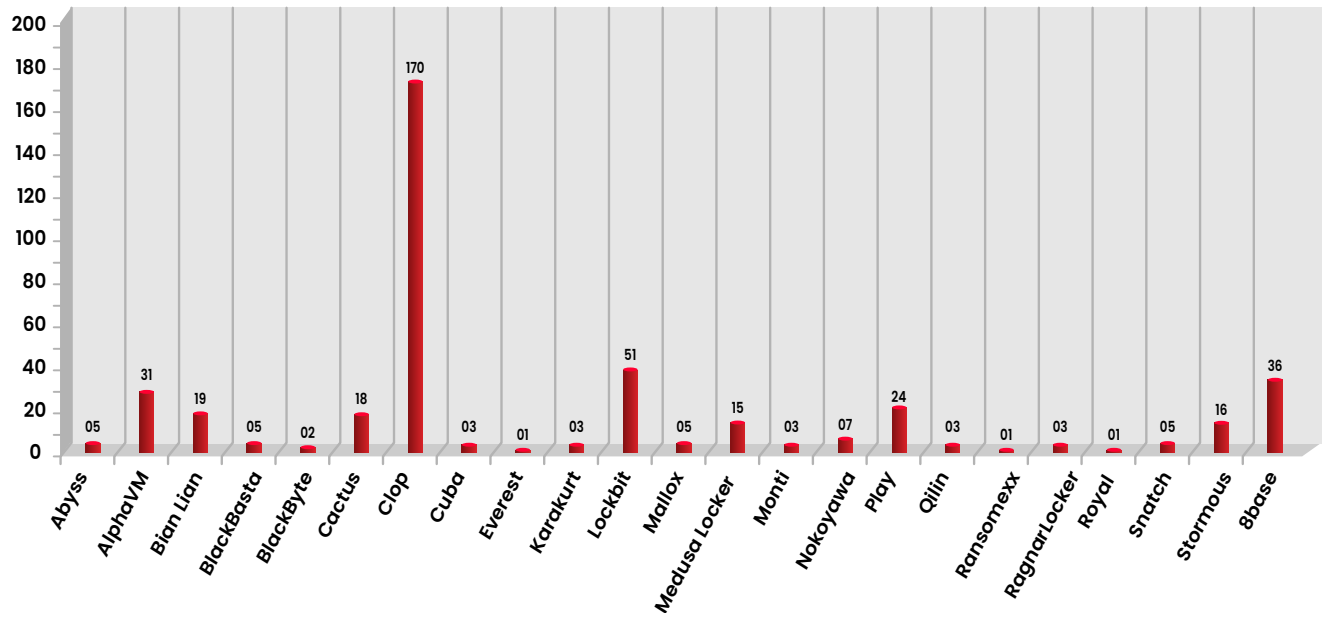
Ransomware Statistics

- Clop ransomware continues to wreak havoc for the second month with more than 150 victims.
- Major victims include Honeywell, Delloitte, Informatica etc.
- Increase in attack rate for India, 9 victims observed mainly by Bian Lian and Clop ransomware.
- Stormous ransomware targets Cuban Government entities.

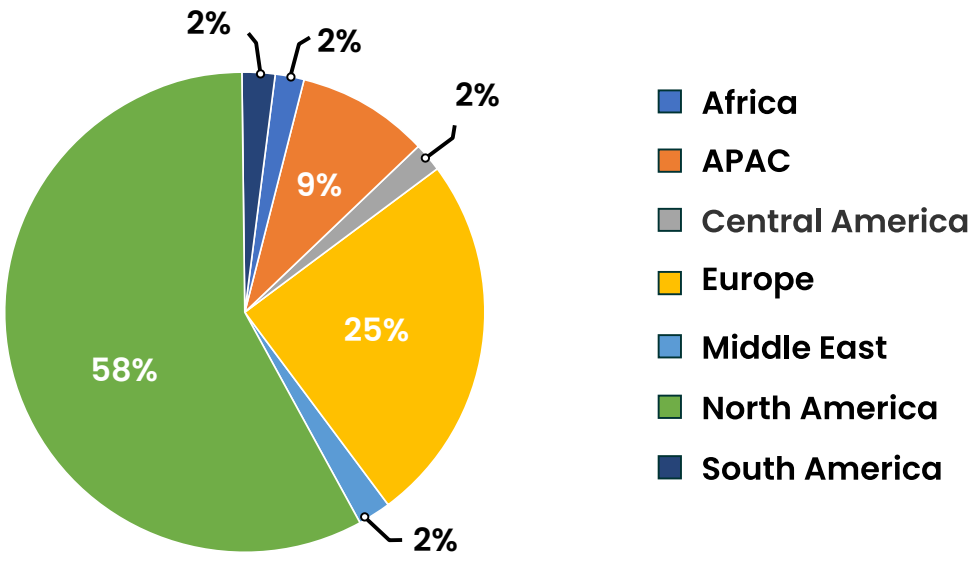
SECTOR-WISE ATTACK TREND



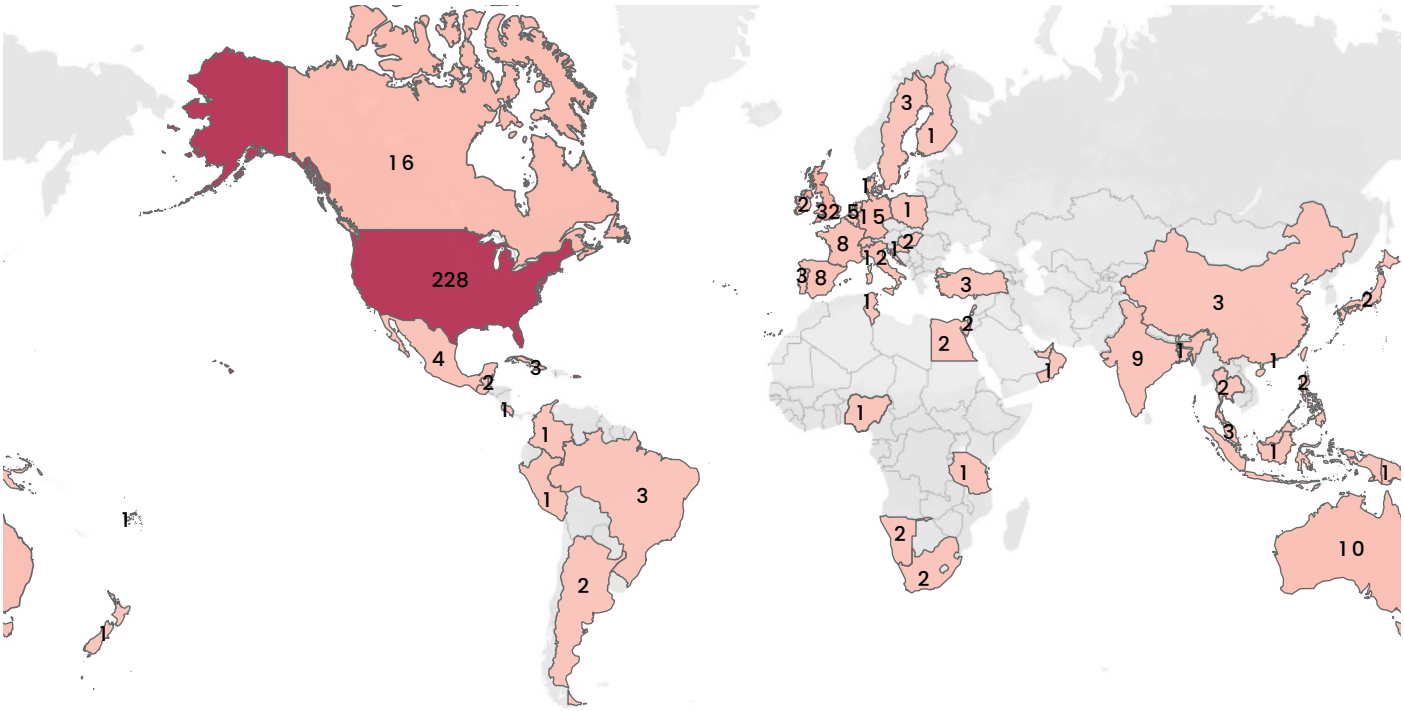
ATTACKS TREND BY RANSOMWARE



REGION-WISE ATTACK



COUNTRY-WISE ATTACK TREND - 424



02

Rising Threat of Mallox Ransomware, Expanded Activities

Tags: Mallox Ransomware, MS-SQL, PowerShell

Mallox, a ransomware strain active since 2021, exploits unsecured Microsoft Windows MS-SQL servers. According to researchers from Unit 42, Mallox activities have surged nearly 174% compared to the previous year, posing an escalating threat. The ransomware uses brute-force attacks and data exfiltration tactics, following the trend of double extortion. It gains unauthorized access to data, encrypts it, and then threatens to leak the stolen data if the ransom is not paid.

The attack begins with a dictionary brute-force attack on unsecured MS-SQL servers. Once they gain access, the attackers use a command line and PowerShell to download the ransomware payload from a remote server. Before encryption, the ransomware tries multiple actions to ensure the successful execution of its payload.

Initially, Mallox was a small, closed group. However, according to a member's statement in January 2023, there are signs that the group is expanding its operations. It appears to be recruiting affiliates on hacking forums, indicating a potential increase in its operational capacity. This growing threat underscores the importance of robust cyber defence mechanisms and frequent software updates to secure MS-SQL servers.

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

03

APT41 Exploits Android Mobile Phones Via WyrmSpy and DragonEgg

Tags: Android, APT41, Wyrmspy, DragonEgg

The Chinese threat group APT41, also known as Double Dragon, BARIUM, and Winnti, has been linked by Lookout to two advanced Android surveillance-ware, WyrmSpy and DragonEgg. Although APT41 is mostly recognized for exploiting web applications and traditional endpoint devices, these instances represent rare mobile platform exploits. A connection between WyrmSpy and DragonEgg was established through the use of overlapping Android signing certificates. WyrmSpy served as the key to link the malware to APT41 due to a tie-in with the command-and-control (C2) infrastructure and Chengdu 404.

WyrmSpy primarily masquerades as a standard Android system app or other service apps, while DragonEgg is found in apps impersonating third-party Android keyboards and messaging apps like Telegram. By mimicking legitimate apps, APT41 gains extensive access to device data, including contacts, SMS messages, location, audio recordings, and camera photos, while staying undetected.

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

04

FIN8 Group Exploits POS Devices Using Noberus Ransomware and Sardonic Backdoor

Tags: BFSI, POS devices, FIN8, Syssphinx, Noberus

Symantec's Threat Hunter Team recently observed the FIN8(aka Syssphinx) cybercrime group, initially known for point-of-sale (POS) attacks, using a variant of the Sardonic backdoor to deliver the Noberus ransomware. This move suggests Syssphinx's shift towards diversifying its attack methods to maximize profits. The group was first observed using ransomware in its attacks in June 2021, when it deployed the Ragnar Locker ransomware developed by a financially driven cybercrime group, Hornworm, also known as the Viking Spider.

In January 2022, Syssphinx was linked to the White Rabbit family of ransomware for using a variant of the Sardonic backdoor, one of its known tools. By December 2022, the group was seen attempting to deploy the Noberus ransomware, operated by the financially motivated cybercrime group Coreid, also known as Blackmatter, Carbon Spider, and FIN7.

Syssphinx is known for taking extended breaks between attack campaigns to refine its tactics, techniques, and procedures (TTPs), reflecting in its December 2022 attack. The group's evolution from POS attacks to ransomware deployments signifies its commitment to maximizing profits, periodically refining its tools and tactics to avoid detection, and making it a significant threat to organizations.
For IOCs, refer to **Appendix 1C.**

05

Use of AI by Threat Actors Simplified by WormGPT and FraudGPT

Tags: Dark web, Fraud GPT, Worm GPT, BEC

WormGPT, an AI module built on the GPTJ language model, has demonstrated significant potential for sophisticated phishing and Business Email Compromise (BEC) attacks. Equipped with numerous features like unlimited character support, chat memory retention, and code formatting capabilities, it was primarily trained on malware-related data. In an experiment, WormGPT crafted an alarmingly persuasive email aimed at tricking an account manager into paying a fake invoice.

Another tool of concern is FraudGPT, an AI bot specifically designed for offensive purposes, such as generating spear phishing emails and creating cracking tools. Sold on Dark Web marketplaces and the Telegram platform, it can produce highly convincing emails that increase the likelihood of recipients clicking on malicious links, thereby boosting the success of BEC phishing campaigns. Subscription fees for FraudGPT range from $200 per month to $1,700 per year.

FraudGPT's features include the ability to write malicious code, create undetectable malware, identify non-VBV bins, construct phishing pages and hacking tools, find "cardable" sites, and detect vulnerabilities. It's marked by over 3,000 confirmed sales and reviews, and offers 24/7 escrow services, highlighting its widespread use and potential risks.

06

Microsoft Thwarts Storm-0558's Attack on Azure AD and Outlook Infrastructure

Tags: Microsoft, Azure AD, Outlook, Storm-0558

China-based threat actor, Storm-0558 was found to be using forged authentication tokens to gain unauthorized access to user emails from around 25 organizations, including government agencies and public cloud consumer accounts, starting May 15, 2023. Microsoft successfully blocked this espionage campaign and notified all impacted or targeted customers. The company has identified the root cause, disrupted malicious activities, hardened the environment, and coordinated with government entities since the detection of this malicious campaign on June 16, 2023.

Storm-0558 is believed to be a distinct group, despite some overlap with other Chinese groups like Violet Typhoon. Its primary targets have been the US and European diplomatic, economic, and legislative governing bodies, as well as individuals connected to Taiwan and Uyghur geopolitical interests.

The threat actor acquired an inactive Microsoft Account (MSA) consumer signing key and used it to forge authentication tokens for Azure AD enterprise and MSA consumer accounts to access email applications. Although the key was intended only for MSA accounts, a validation issue allowed the key to be trusted for signing Azure AD tokens. Microsoft has since invalidated all MSA keys active prior to the incident.

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

07

Critical Vulnerabilities Identified in Rockwell Automations ControlLogix Systems

Tags: ICS/OT, CVE-2023-3595, CVE-2023-3596

Advanced Persistent Threat (APT) actors have been linked to a new exploit capability affecting specific Rockwell Automation ControlLogix EtherNet/IP (ENIP) communication module models. This exploit allows remote code execution with persistence and denial of service (DoS) attacks on the devices. Dragos, an ICS/OT threat intelligence vendor, identified and shared the vulnerabilities with ControlLogix.

The affected communication modules are integral to ControlLogix systems in numerous industrial sectors like manufacturing and energy. The vulnerabilities, listed as CVE-2023-3595 and CVE-2023-3596, exist in the devices' Common Industrial Protocol (CIP) implementation and can lead to arbitrary firmware memory manipulation, denial or loss of control, and theft of operational information.

The impact is reminiscent of the zero-day employed by XENOTIME in the TRISIS attack, as they both allow for memory manipulation and potentially compromising incident response and recovery information. As of mid-July 2023, no evidence of exploitation in the wild has been found, but the situation could change, posing a serious risk to customers using affected products.

08

A Mexican Threat Actor-Neo_Net Targeting Global Banks in Recent Campaign

Tags: BFSI, Malware, Campaign

An elaborate eCrime campaign discovered by a researcher at QuoIntelligence and published on SentinelOne, has been operational from June 2021 to April 2023, and targeted clients of major banks worldwide, primarily focusing on Spanish and Chilean institutions such as Santander, BBVA, and CaixaBank. Orchestrated by a cybercriminal known as Neo_Net, the operation resulted in over 350,000 EUR being stolen from victims' accounts and compromising a significant volume of personal data. Neo_Net established an expansive infrastructure for this campaign, renting out phishing panels, Smishing software, and Android trojans to various affiliates.

The operation commenced with SMS phishing messages distributed across Spain, creating an illusion of legitimacy through mimicked Sender IDs of reputable banks. The phishing pages were expertly crafted, appearing identical to genuine banking applications, and victims' information was covertly channelled to a Telegram chat. The stolen data enabled the threat actors to bypass Multi-Factor Authentication (MFA) and compromise accounts.

Neo_Net, traced back to Mexico and primarily operating in Spanish-speaking countries, also collaborated with non-Spanish speakers in further cybercrimes, including Google Ads operations targeting crypto wallet owners.

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

09

Rustbucket Targets MacOS Users

Tags: MacOS, Rustbucket

The Elastic Security Labs team has detected a novel variant of the RUSTBUCKET malware family, previously associated with the BlueNorOff group by Jamf Threat Labs. This new variant targets macOS systems, displaying unique persistence capabilities unseen in prior iterations. Furthermore, this variant remains undetected by VirusTotal signature engines while the research was performed by Security Labs, indicating the malware family is still actively developed.

The process of infection begins with the execution of an AppleScript using the /usr/bin/osascript command, initiating the download of the Stage 2 binary from the command-and-control (C2) network via cURL. The Stage 2 binary, written in Swift, operates based on command-line arguments and anticipates a C2 URL as the initial parameter. It sets the User-Agent string as mozilla/4.0 and includes the string "pw" in the HTTP request's body.

A venture-backed cryptocurrency company in the U.S., identified as REF9135, was targeted, which aligns with the BlueNorOff group's previous behaviour of attacking organizations with considerable cryptocurrency resources. Elastic Defend provides user protection through behavioural and prebuilt detection rules and a new signature to thwart this malware execution.

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

10

VirusTotal Data Leak Exposes Security Researchers

Tags: IT

In a significant data breach identified by German Researchers, a confidential 313-kilobyte file containing 5,600 names, including employees of the US NSA and German secret services, was leaked on the internet in late June, when an employee of VirusTotal unintentionally uploaded a CSV file on the platform. These individuals had registered on VirusTotal, an IT security platform widely respected among cyber-security experts for its pivotal role in combating cyber-attacks. VirusTotal is globally used by IT professionals to check files for viruses, effectively functioning as a vast malware database. Users can upload suspicious files or links, contributing to an extensive archive of digital attack tools akin to a malicious code library. Approximately 70 antivirus software manufacturers utilize VirusTotal to scrutinize submissions for potentially malicious program lines, such as Trojans.

The leak is particularly striking as VirusTotal is a Google-owned entity, a world-leading company renowned for its robust defenses against hacking attempts. There have been few instances of internal data from Google systems being publicly exposed due to a leak, making this event noteworthy.

11

Appendix

APPENDIX 1A - MALLOX RANSOMWARE

SHA256
6c743c890151d0719150246382b5e0158e8abc4a29dd4b2f049ce7d313b1a330
b03f94c61528c9f3731a2e8da4975c072c9ed4e5372d3ec6b0939ee-be01e54a4
de9d3e17555e91072919dc700dc7e588cd52617debcad2f764ef9c7fbf6c9f7b
2a549489e2455a2d84295604e29c727dd20d65f5a874209840ce187c-35d9a439
1c8b6d5b79d7d909b7ee22cccf8f71c1bd8182eedfb9960c94776620e4543d13
36269d1892283991a9db23492cd8efcd68af74060384b9686219a-97f76a9989e
10eea0c13fd1a782c065627e23e7051edc1622f2eae5fbe138725369c12f4b6d
Df30d74ab6600c1532a14c53a7f08f1afd41ec63cf427a4b91b99c3c2524caba
0463277782f9e98b0e7a028cea0f689a81cf080fa0d64d4de8ef4803bb1b-f03a
1f793f973fd906f9736aa483c613b82d5d2d7b0e270c5c903704f9665d9e1185
e284ad63a832123240bd40b6c09565fae8525c00ddf308d5b8f5c-8ce69ed6b09
e3a0bbd623db2b865fc3520c8d05e8b92016af2e535f0808460295c-b8435836a
7c84eafb3b05f0d5316fae610d9404c54ef39383d0fe0e-3c07407a26bb9f6750
1276786fc51f3b7e987aa95ebff0a3e1e358ee4e86e2302e472f84710271af7b

f730e83049c7fe81f6e4765ab91efbb7a373751d51fdafe697a4977dc7c1ea11
05194b34f8ff89facdd7b56d05826b08edaec9c6e444bdc32913e-02cab01afd4
c599bebc9ae54a54710008042361293d71475e5fbe8f0cbace-b6ee4565a72015
060ed94db064924a90065a5f4efb50f938c-52619ca003f096482353e444bd096
90be90ad4fb906574f9e7afe587f0826a71152bfc32cfc665a58877562f2edd4
1b2727af9fc187cd5c932c6defe50b983ad7508b4196ad6c5ff5e96686277c56
a9543bc9612276863fc77b663fa3ff6efb85db69a01baa86c6dfabf73684b5c1
4e00f3e0e09d13e76da56009173098eefaf-c4ad50806583d5333990fa44e6420
6c109d098a1f44017f3937a71628d9dbd4d2ca8aa266656ee4720c-37cc31558e
7f8f1afa1390246409263e606aa05e2896b8d1da7018c534e67ca530a59eb-da1
8e54c38bc3585c3163c3e25d037bcf55695c274aaea770f2f-59f0a0910a4b572
724aa6dae72829e9812b753d188190e16fb64ac6cd39520897d917cfdccc5122
7164ba41639c8edcd9ff1cf41a806c9a23de566b56a7f34a0205ba1f84575a48
0e1c7ea4148e7473e15a8e55413d6972eec6e24ef365e9f629884f89645de71a
4ed74a205fad15c843174d7d8b30ae60a181e79f31cc30ebc683072f187e4cdd
ee6fd436bf5aff181e3d4b9a944bf644076e902a1bbf622978b5e005522c1f77
ebdcf54719cceddffc3c254b0bfb1a2b2c8a136fa207293dbba8110f066d9c51
9a3050007e1c46e226e7c2c27d4703f6396280386329044919 3a0d-0ca9661b3b

d6c51935d0597b44f45f1b36d65d3b01b6401593f95cb-4c2786034072ad89b63
586d4f86615cb3a8709ae1c08dde35087580814c1d1315af3d7b932639ff48e0
8e974a3be94b7748f7971f278160a74d738d5cab2c3088b1492cfbb-d05e83e22
3fa36079fdc548db1b5122450c2e4c9e40c37059de116d1c03f6459b13fc2dc4
D15f12a7cf2e8ec3d6fceabfab64956c7e727caab91cff9c664f92b5c8552570
0427a9f68d2385f7d5ba9e9c8e5c7f1b6e829868ef0a8bc89b2f-6dae2f2020c4
4cbac922af3cfaba5fa7a3251bd05337bffd9ed0ada77c55bb4f78a041f4ebf2
10f96f64659415e46c3f2f823bdb855aab42d0bfced811c9a3b72aea5f22d880
5ccff9af23c18998221f45396732539d18e330454327d1e7450095c682d8c552
77fdce66e7f909300e4493cbe7055254f7992ba65f9b7445a6755d0dbd-9f80a5
ee08e3366c04574f25909494ef276e65e98d54f226c0f8e51922247ca3c-fade9
2fd3c8fab2cfaaabf53d6c50e515dd5d1ef6eceeebdd5509c23030c4d-54cb014
603846d113ef1f588d9a3a695917191791fbad441f742bcfe797813f9fc5291e
a5085e571857ec54cf9625050dfc29a195dad4d52bea9b69d-3f22e33ed636525
9b833d5b4bdbc516e4773c489ced531b13028094ce610e96ebc-30d3335458a97
b9e895830878124e20293f477549329d4d8752ff118f4fe893d81b3a30852c0b
cd80506f971b95b3b831cef91bb2ec422b1a27301f26d5deac8e19f163f0839a
c0e35b19f97021416e3724006511afc95d6aa409404e812d8c62b955bc917d3c

342930d44aed72f826a3f0f4a3964158f2bd86fb53703fb3daa6c-937b28a53e4
9ee35c6eb97230cd9b61ba32dba7befea4122f89b-3747d2389970050a1d019f9
e7e00e0f817fcb305f82aec2e60045fcdb1b334b2621c09133b6b81284002009
e3f63ab8ef91e0c52384c0e3e350db2427c8cb9237355800a3443b341cf-8cf4f
f7e8a0eac54dd040e2609546fca263f2c2753802ff57e7c62d5e9ccfa04bd-b1a
e7178a4bad4407316b85894307df32fdf85b597455364eb8ec-4d407749e852ce
dcc9e23fd6ac926eb9ee7e0ee422dacd2059b4a42c8642d32bdf4f5c8eb-33f6a
fead3d518752ddb4d2407f16ca5f3c9b3c0bf01972a2618369d02913f7c6af1a
0901a9920c9f0c74fb2170524477693d62c8493715520ae95143ab-d8055e7a39
ba97fd533e8a552664695434227b24ca1e2e661c360a7a0a40ff59ba6b-8fe949
53da732df7599f5ad21a26b669500788a827f3a8358dcdca10997d2b-8187c95c
189c9c4603defb14fa8c942f5ff781480465426991764047868653 0f91c4b66c
fd0030883b9e74b383ee6381a2aaa7e2e5b93a00003b555e2f7c8b7be-65ab176
d22b3218c4b7f13fe114854d1dbda02c3ad94a1b6c69daa1cf6a504ada8b8b-ca
b6447b0636085fcb41fd574e84500958f21dfe87fe06b0813fb9399d63f28851
5c34f6fa6eada3197404bf95eced9d28868853759862915 8a4f4e18d-6882cb9b
d81b0425d4ec49bad194b8dc750524c2a29994fe972e733376349f47961c-fa62

IPs
103.96.72[.]140
80.66.75[.]36
80.66.75[.]37
80.66.75[.]126
80.66.75[.]116
92.118.148[.]227
62.122.184[.]113
87.251.64[.]245
119.3.125[.]197
49.235.255[.]219
80.66.75[.]55
87.251.67[.]92
121.4.69[.]26
124.223.11[.]169
45.93.201[.]74
80.66.75[.]135
194.26.135[.]44
80.66.75[.]51
89.117.55[.]149
5.181.86[.]241
185.170.144[.]153

Appendix 1B – APT41, WyrmSpy and DragonEgg

SHA1
92ddbe438c8c8c1ef82fa5bb02e526db10829736
0b4a9a3f167178054ef9f9a97463cbe31f078c2f
d713b8b0f3764157cc18d5dc1cb0f9c558067728
589d88093dad377d46f34415a7f9df11d65b81ed
ab560af6bafff8f58ea5bc53c0391501415aed14
5891fa6a3a8232192ebd57a171bad29f53c7598c
4405af38c4a6b6130fcf242a11b0ce7963a1be28
5c16637848d6f1eb4aa6c5b2a4928a1144cd2113
2fbd56b1f3859c6d03dec47f8fcee7e37dc303a1
085191fb59d3933f8447610126600754b35697d4
d634a548973c7931e224a41201be0a273d561cff
971f4cd569ad9f84e654b62bffdba3a4aa21d4e9
331acbdd270acecfa80bc7b4e37629611593de0a
215847e4c41144365b94cb924d969dbc5e69052b
cc351ffbe748b1db43de6dcd40934fe23986e753
85ca8cd21d70668bd2aab9c53163f5e03a0e1a8b
6dd20f7b9ccbd961d155fff78452303a54714841
d02f548d354adff645318de6edc45dff23170241
2438069c43771f0011da2f22b57b8336aaa7562c
5c2fc57609ee28753b78a0f33ba7519fc9fbb6f8
53c745956c3501d1daf232aeea5edfb52168c6b4
dfff9ae245cc0beed8fdf409c00ec758d7d2678f

517ec909bc9e308b44d59dfd144188d1e23f57bc
232b868e36f064b4151e4386835642fc8bf07e0b
92ddbe438c8c8c1ef82fa5bb02e526db10829736
9b6297825a6c00b3af16748684d4de551cc7be75
0b4a9a3f167178054ef9f9a97463cbe31f078c2f
d713b8b0f3764157cc18d5dc1cb0f9c558067728
589d88093dad377d46f34415a7f9df11d65b81ed
ab560af6bafff8f58ea5bc53c0391501415aed14
5891fa6a3a8232192ebd57a171bad29f53c7598c
e514042565ffb2811f780227fee5ed5683925d49
4405af38c4a6b6130fcf242a11b0ce7963a1be28
17e6bbed5e43ec5b8d2821e0145da7ee32a58ea6
5c16637848d6f1eb4aa6c5b2a4928a1144cd2113
2fbd56b1f3859c6d03dec47f8fcee7e37dc303a1
085191fb59d3933f8447610126600754b35697d4
d634a548973c7931e224a41201be0a273d561cff
971f4cd569ad9f84e654b62bffdba3a4aa21d4e9
331acbdd270acecfa80bc7b4e37629611593de0a
58cda5e4607557d79bc5e36764b577f17e77af49
a9d2f59b8457c6998b654054084b102adfcf3306
215847e4c41144365b94cb924d969dbc5e69052b
cc351ffbe748b1db43de6dcd40934fe23986e753
85ca8cd21d70668bd2aab9c53163f5e03a0e1a8b
6dd20f7b9ccbd961d155fff78452303a54714841

d02f548d354adff645318de6edc45dff23170241
2438069c43771f0011da2f22b57b8336aaa7562c
5c2fc57609ee28753b78a0f33ba7519fc9fbb6f8
53c745956c3501d1daf232aeea5edfb52168c6b4
b456a61a3e0ac6073a716b06293a3295a261de56
209567f4f28c5c8abcbe56d789e558aa64239534
b456a61a3e0ac6073a716b06293a3295a261de56
cab70e99516a36ab0f0d3851375adf0740f4bd5e
81762cfae0bd5585e8c0c86e4fdbbe47d2dd614a
fbda76a2c2834f89d642a72c24b1988a1f56e4b8

Network
116.205.4[.]18
dns.win10micros0ft[.]com
www.andropwn[.]xyz
121.42.149[.]52
update.umisen[.]com
118.193.39[.]165
121.201.109[.]98
alxc.tbtianyan[.]com
yxwasec[.]com
smiss.imwork[.]net
huaxin-bantian.duckdns[.]org
103.43.17[.]99

Appendix 1C – FIN8

Network
37.10.71[.]215 – C&C server
api-cdn[.]net
git-api[.]com
api-cdnw5[.]net
104-168-237-21.sslip[.]io

SHA-256
1d3e573d432ef094fba33f615aa0564feffa99853af77e10367f54dc6df95509 – PowerShell script
307c3e23a4ba65749e49932c03d5d3eb58d133bc6623c436756e48de68b-9cc45 – Hacktool.Mimikatz
48e3add1881d60e0f6a036cfdb24426266f23f624a4cd57b8ea945e-9ca98e6fd – DLL file
4db89c39db14f4d9f76d06c50fef2d9282e83c03e8c948a863b58ded-c43edd31 – 32-bit shellcode
356adc348e9a28fc760e75029839da5d374d11d-b5e41a74147a263290ae77501 – 32-bit shellcode
e7175ae2e0f0279fe3c4d5fc33e77b2bea51e0a7ad29f458b609af-ca0ab62b0b – 32-bit shellcode
e4e3a4f1c87ff79f99f42b5bbe9727481d43d68582799309785c95d1d0de789a – 64-bit shellcode
2cd2e79e18849b882ba40a1f3f432a24e3c146bb52137c7543806f22c617d62c – 64-bit shellcode
78109d8e0fbe32ae7ec7c8d1c16e21bec0a0da3d58d98b6b266fbc53bb-5bc00e – 64-bit shellcode
ede6ca7c3c3aedeb70e8504e1df70988263aab60ac664d03995b-ce645dff0935

5b8b732d0bb708aa51ac7f8a4ff5ca5ea99a84112b8b22d13674da7a-8ca18c28
4e73e9a546e334f0aee8da7d191c56d25e6360ba7a79dc02fe93efbd41f-f7aa4
05236172591d843b15987de2243ff1bfb41c7b959d7c917949a7533ed60aafd9
edfd3ae4def3ddffb37bad3424eb73c17e156ba5f63fd1d651df2f5b8e34a6c7
827448cf3c7ddc67dca6618f4c8b1197ee2abe3526e27052d09948da2b-c500ea
0e11a050369010683a7ed6a51f5ec320cd885128804713bb9df0e056e29d-c3b0
0980aa80e52cc18e7b3909a0173a9efb60f9d406993d26fe3af-35870ef1604d0
64f8ac7b3b28d763f0a8f6cdb4ce1e5e3892b0338c9240f27057dd9e087e3111
2d39a58887026b99176eb16c1bba4f6971c985ac9acbd9e2747d-d0620548aaf3
8cfb05cde6af3cf4e0cb025faa597c2641a4ab372268823a29baef-37c6c45946
72fd2f51f36ba6c842fdc801464a49dce28bd851589c7401f64bbc4f1a468b1a
6cba6d8a1a73572a1a49372c9b7adfa471a3a1302dc71c4547685bcbb1e-da432

Appendix 1D – Storm-0558

IPs
51.89.156[.]153
176.31.90[.]129
137.74.181[.]100
193.36.119[.]45
185.158.248[.]159
131.153.78[.]188
37.143.130[.]146
146.70.157[.]45
185.195.200[.]39
185.38.142[.]229
146.70.121[.]44
31.42.177[.]181
185.51.134[.]52
173.44.226[.]70
45.14.227[.]233
185.236.231[.]109
178.73.220[.]149
45.14.227[.]212
91.222.173[.]225
146.70.35[.]168
146.70.157[.]213
31.42.177[.]201

5.252.176[.]8
80.85.158[.]215
193.149.129[.]88
5.252.178[.]68
116.202.251[.]8
185.158.248[.]93
20.108.240[.]252
146.70.135[.]182

Appendix 1E – Neo_Net

Network
bbva.info-cliente[.]net
santander.esentregas[.]ga
bbva.esentregas[.]ga
correos.esentregas[.]ga

Appendix 1F – Rustbucket

Network
webhostwatto.work[.]gd
crypto.hondchain[.]com
starbucls[.]xyz
jaicvc[.]com
docsend.linkpc[.]net
companydeck[.]online
104.168.167[.]88
64.44.141[.]15

Appendix 1E – Neo_Net

SHA-256
9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747
7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387
ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41
de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500
4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16
fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69
7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca-3ce8d25b8

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.