Payatu

December 2022

Cyber Threat Intelligence Report

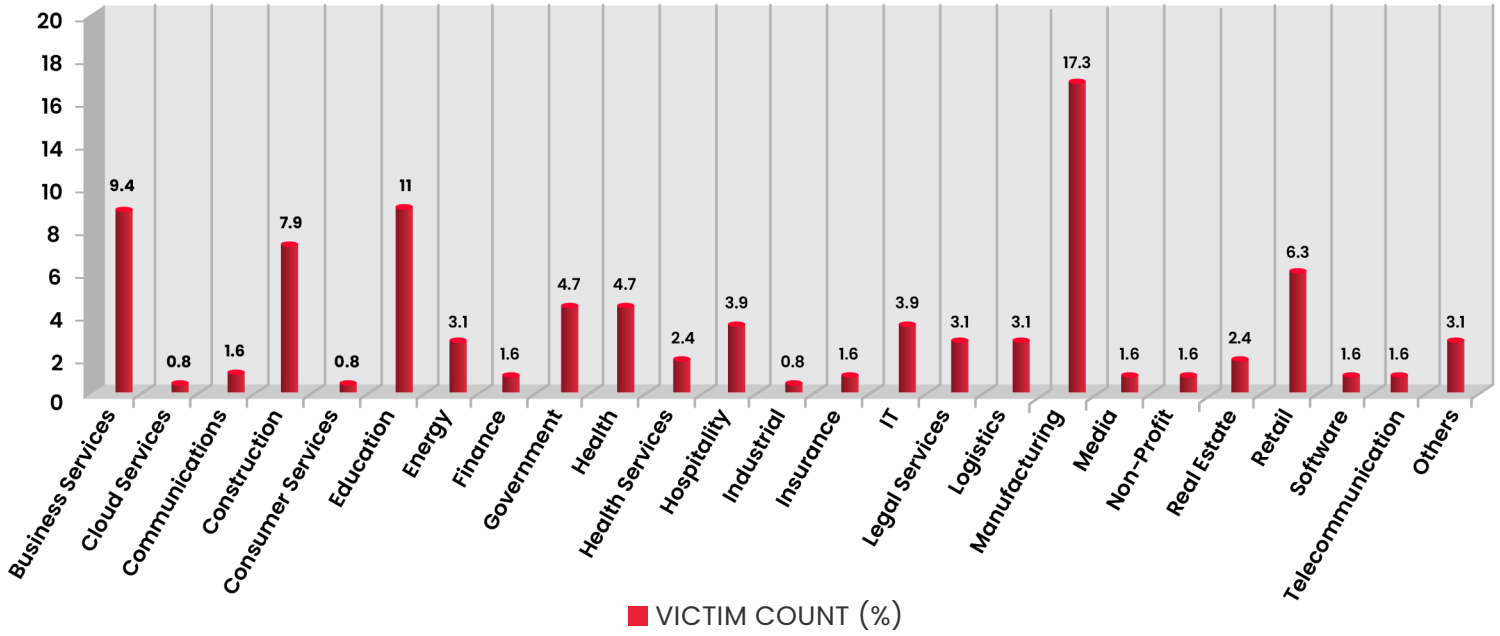
Payatu Security Consulting Pvt. Ltd.

Table of Contents

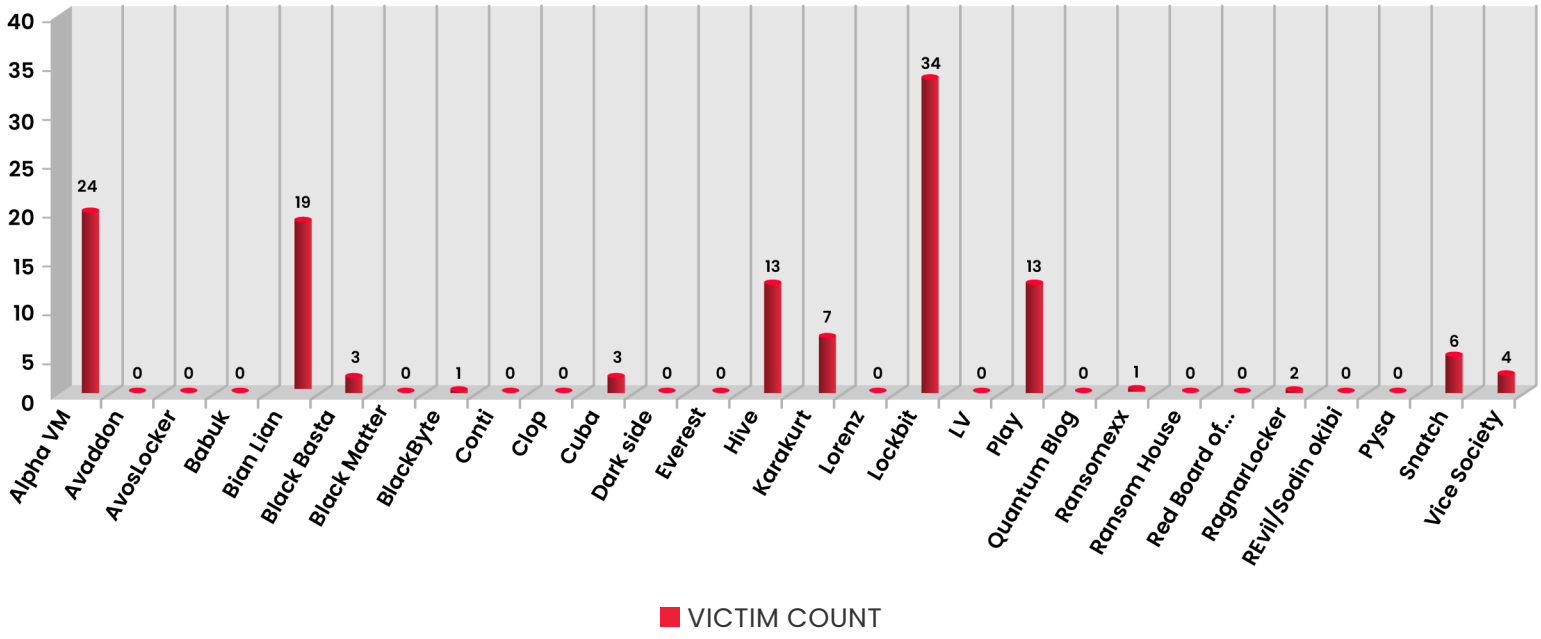
01

Ransomware Statistics

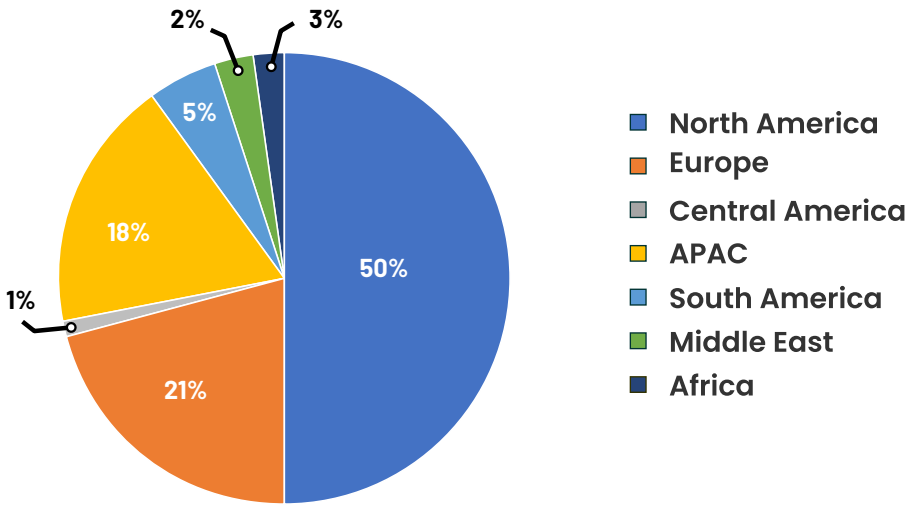
SECTOR-WISE ATTACK TREND



ATTACK COUNT



REGION-WISE ATTACKS TREND



Country-wise Attacks Trend - 131

 Argentina - 2

 Brazil - 5

 Colombia - 1

 China - 1

 Costa Rica- 1

 Cyprus- 1

 France - 3

 Greece - 1

 India - 4

 Italy - 3

 Japan - 2

 Lebanon - 1

 Mexico - 2

 New Zealand - 5

 Norway - 1

 Philippines - 1

 Portugal - 3

 Singapore - 1

 Sweden - 1

 Switzerland - 1

 Taiwan - 3

 United Kingdom - 3

 United States - 52

 Venezuela - 2

02

“In The Box”, The New Haven for Mobile Malware Sellers

Tags: Darkweb, Marketplace, Mobile Trojans, Malware

With an increase in the frequency of cyber-attacks with financial motives in the past couple of years, especially with social distancing, there has been an increase in the effective use of online banking. We saw various malware such as Cerberus, Hydra, Ursnif, Drinik being created and a few older players like Emotet, Trickbot being placed in the wild to infect customers of various financial institutions with the target of compromising devices. In this conquest, the latest addition to the unique world of financial frauds is a dark web marketplace specifically for mobile-based web injects to sell and promote such malware.

As the techniques involved in the attack by these malware compromises devices completely, they can intercept SMS, and hence two-factor authentication (2-FA) is also compromised. In the Box is unique, as the website requires some actions to be performed by a user, as the moderator requires the new users to connect with the administrator over telegram and jabber IDs.

The marketplace hosts various web inject templates such as “Credit Card Data”, “Only PIN”, “Authorization Data”, and “Full Data”; through which a system can be compromised. Customized, based on financial institutions and geography, the website hosts a list of web injects for payment systems like PayPal, Coinbase, Binance, and WazirX; e-Commerce sites like Amazon, Shein, and Alibaba; social media and digital media like Zoom, Instagram, Tinder, Netflix, and Spotify. It also has lists of banks, separated country-wise - USA [Citi Mobile, Amex, Bank of America, etc.].

03

Europe, APAC Realize a New Target on Their Back Amidst Russia-Ukraine War

Tags: Mustang Panda, APAC, China, Phishing Campaign

Amidst Russia-Ukraine war, the Chinese cyber espionage threat actor Mustang Panda has been observed to be exploiting the geopolitical scenario to its advantage. Luring people with phishing campaigns revolving around EUs approach towards Russia, the threat group shares a RAR (WINRAR) file to deliver PlugX payload, Blackberry researchers share in a threat intelligence report.

Disguised in a doc-based shortcut file, the payload gets executed on-click, followed by defining location/environment of executable – "ClassicExplorerSettings.exe" and attempting to execute the DLL file. Here, another payload is implanted in order to perform DLL side-loading, a technique very often used by the group. The purpose of the DLL upload is to load a DAT file containing shell code within.

Executed payloads connect to Command & Control server hosting an SSL certificate which assists in identifying 15 other suspicious IP addresses. The targets as per the team are believed to be Southeast Asia (specially Vietnam, India, Myanmar), European Union, parts of Africa and South America.

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

04

Updated Techniques of Iran's MuddyWater Threat Group

Tags: Iran, MuddyWater

Not only in the real-world warfare techniques, but the month of December also saw an update in the cyber warfare techniques that are attributed to Iran's Ministry of Intelligence and Security (MIOS) related entity – MuddyWater aka Static Kitten. Researchers at DeepInstinct presented a report on the same, highlighting targets and techniques used by the group lately.

Actively targeting countries like Armenia, Azerbaijan, Egypt, Iraq, Israel, UAE; the group previously used spear-phishing emails with links (T1566.002) and attachments (T1566.001) containing archived legitimate Remote Administration Tool – RemoteUtilities and Screen Connect. However, recent activities observe a new remote administration tool – Syncro being used. Previously named as random strings, MSI (Microsoft Installer) package containing ScreenConnect and Syncro is now named after legitimate Saudi-based organization – "Ertiqa.msi".

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

05

Open-source Malicious Packages, a New Threat to Developers Supply Chain

Tags: PyPi, NPM, NuGet, Golang, Python, Ransomware

With an increase in the use of open-source tools and packages for developing new technologies, without verifying the packages as was a traditional practice when *nix systems published packages and their SHA256 values to make sure that the packages the community used were legitimate. The resultant attack vector that is being developed as a result of this negligence is seen by various methods.

In one instance, typo-squatting package names of PyPi like requests [dequests, rewuests, req7ests] and NPM packages observed by team at Phylum, observed the typosquatted packages making an outgoing connection to download binaries as per Operating System. The binaries are attributed to the ransomware, demanding $100 in BTC, ETH, etc. for the decryption key.

Another instance observed by Checkmarx is a massive push in malicious packages (~144K) which are a part of phishing campaign wherein automated scripts create packages with generic name patterns as suggested by NuGet publication. With over 90 phishing domains in these packages, the attackers lure users into clicking the links by defining names as cheats, hacks and free sources for some commercial applications/ products.

In another instance, it was the SentinelOne PyPi modules posing as SDKs (Software Development Kits) appearing like legitimate SentinelOne packages, reported by ReversingLabs. The package also uses typosquatting as the technique to exploit developers and push malicious code into pipelines, endangering the entire supply chains.

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

06

Leaked Secrets? GitHub to the Rescue

Tags: Github, Passkey, Secretkey

Often it happens that while publishing a useful tool or code with the purpose of assisting the developing community, that developers miss out on removing sensitive parts of the code such as keys, inclusive of AWS keys, passkeys, account passwords etc. resulting in malicious attackers collecting such information and using it to exploit organizations.

GitHub has introduced a new “secret scanning partner program” that allows organizations to search through the wide database of publicly available repositories, searching for more than 200 different token formats. The identified secrets are available under “Code Security & Analysis” settings.

07

Godfather: New But Old

Tags: Godfather, Anubis, Banking Trojan, Android

Anubis, a well-known Android banking trojan exploited many devices and assisted many attackers to collect and sell credentials including, but not limited to financial institutions, went out of date after some time as the functionalities of the malware became outdated with Android updates and in 2019 its code was leaked.

With basic functionalities like Anubis', a new banking trojan named Godfather is being utilized by cybercriminals in order to compromise their targets and disrupt financial structures. The malware allows threat actors to harvest login credentials for banking applications and other financial services. It has targeted more than 400 banking applications, crypto wallets, and exchanges and has been active since June 2021, suggest researchers at Group-IB. Malware developers have used Anubis' source code as the basis of Godfather, modernizing it against newer versions of Android, and it is a Malware-as-a-Service model.

The malware is distributed through decoy applications hosted on Google Play Store and is also capable of exfiltrating SMS and push notifications. In addition, its functionalities also include recording victims' device's screen, launching keyloggers, bypassing 2FA through exfiltrating SMS and push notifications, and forwarding calls.

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

08

Yet Another Data Breach at Okta, This Time it's the Source Code

Tags: Okta, Github

On 21st December 2022, Okta updated its users about a security breach, that occurred in early December 2022, due to suspicious access to Okta's code repositories as reported by Github to the team. After due investigation, the team identified access to a copy of Okta's source code, concluding that no unauthorized access to customer data or service was observed, it also suggested that Okta does not rely on its source code confidentiality.

09

New Botnet Targets WordPress Admins

Tags: Botnet, WordPress, Golang

Researchers at Fortinet have identified a new Go-based botnet, named GoTrim, that has been targeting Admin accounts of WordPress websites, brute forcing passwords through a tool written in Golang. By affecting Linux based platforms, the attackers can gain control of the vulnerable systems remotely.

The attacker sends out brute force commands to initialize the attack through its Command & Control (C2) server, which in turn sends out the list of brute force combinations to the bots (i.e., compromised systems) to attempt logins on multiple websites using given credentials. Once this process is completed, the next step is to push PHP scripts and elf files to the target system.

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

10

Massive Data Breach at BitKeep

Tags: Bitkeep, Data breach, Cryptocurrency, Cryptowallet

On 28th December 2022, Bitkeep updated its customers about a data breach compromising cryptocurrencies worth $8 million. According to Bitkeep, a hacker exploited and compromised Bitkeep 7.2.9 APK and implanted a malicious code leading to leak of private keys of users enabling hackers to move funds to their accounts. The application hosted on Google Playstore and iOS App Store remain safe as the compromise occurred at the downloadable version hosted on Bitkeeps' official website and any third-party websites which hosted the file from there.

As per the company, the fund movement was stopped saving $7 million transactions, while $1 million were lost. As a way forward, the company has updated a fresh version to their websites and requests all users compromised, to generate new wallet addresses as the previous addresses and keys remain affected.

11

Appendix

Appendix 1A – Mustang Panda

SHA256
f70d3601fb456a18ed7e7ed599d10783447016da78234f5dca61b8bd3a084a15

Appendix 1B – Revil Ransomware

C2
5[.]34.178.156
104[.]42.43.178
64[.]34.216.50
45[.]147.26.45
45[.]32.101.7
64[.]34.216.44
185[.]80.201.4
103[.]192.226.87
194[.]124.227.90
43[.]254.218.128
62[.]233.57.49

Appendix 1B – MuddyWater

SHA256
f511bdd471096fc81dc8dad6806624a73837710f99b76b69c6501cb90e37c311
efd5271bdb57f52b4852bfda05122b9ff85991c0600befcbd045f81d7a78eac5
d65d80ab0ccdc7ff0a72e71104de2b4c289c02348816dce9996ba3e2a4c1dd62
1670a59f573037142f417fb8c448a9022c8d31a6b2bf93ad77a9db2924b502af

dedc593acc72c352feef4cc2b051001bfe22a79a3a7852f0daf95e2d10e58b84
eae0acba9c9e6a93ce2d5b30a5f21515e8ccca0975fbd0e7d8862964fdfa1468
7e7292b5029882602fe31f15e25b5c59e01277abaab86b29843ded4aa0dcbdd1
c7a2a9e020b4bcbfa53b37dea7ebf6943af203b94c24a35c098b774f79d532ac
887c09e24923258e2e2c28f369fba3e44e52ce8a603fa3aee8c3fb0f1ca660e1
01dfa94e11b60f92449445a9660843f7bea0d6aad62f1c339e88252008e3b494
d550f0f9c4554e63b6e6d0a95a20a16abe44fa6f0de62b6615b5fdcdb82fe8e1
61dcf1eeb616104742dd892b89365751df9bb8c5b6a2b4080ac7cf34294d7675
c6cfd23282c9ff9d0d4c72ee13797a898b01cd5fd256d347e399e7528dad3bfd
5578b7d126ebae78635613685d0cd07f4fb86f2e5b08e799bdc67d6d6053ede2
32339f7ac043042e6361225b594047dd4398da489a2af17a9f74a51593b14951
dab77aea8bf4f78628dcf45be6e2e79440c38a86e830846ec2bddc74ff0a36e4
b5c7acf08d3fd68ddc92169d23709e36e45cb65689880e30cb8f376b5c91be57
2a5f74e8268ad2d38c18f57a19d723b72b2dadd11b3ab993507dd2863d18008d
e87fe81352ebda0cfc0ae785ebfc51a8965917235ee5d6dc6ca6b730eda494cf
aa282daa9da3d6fc2dc6d54d453f4c23b746ad5b295472e7883ee6e6353b671
4e80bd62d02f312b06a0c96e1b5d1c6fd5a8af4e051f3f7f90e2976580842515
697580cf4266fa7d50fd5f690eee1f3033d3a706eb61fc1fca25471dbc36e684
dc7e102a2c68f7e3e15908eb6174548ce3d13a94caadf76e1a4ee834dc17a271
f24ce8e6679893049ce4e5a03bc2d8c7e44bf5b918bf8bf1c2e45c5de4d11e56
433b47f40f47bea0889423ab96deb1776f47e9faa946e7c5089494ed00c6cc29
011cb37733cdf01c689d12fedc4a3eda8b0f6c4dcdeef1719004c32ee331198e
e217c48c435a04855cf0c439259a95392122064002d4881cf093cc59f813aba8
331b513cf17568329c7d5f1bac1d14f38c77f8d4adba40c48dab6baf98854f92
4d24b326d0335e122c7f6adaa22e8237895bdf4c6d85863cf8e84cfcc0503e69
a35a1c92c001b59605efd318655d912f2bcd4e745da2b4a1e385d289e12ee905
4550b4fa89ff70d8ea59d350ad8fc537ceaad13779877f2761d91d69a2c445b2
653046fa62d3c9325dbff5cb7961965a8bf5f96fa4e815b494c8d3e165b9c94a
76ab046de18e20fd5cddbb90678389001361a430a0dc6297363ff10efbcb0fa8

Appendix 1C – Malicious Open-source Packages

MD5	EXE files
a227bc1e67b3fee42f6236f858d75269e2e684db	cia.windows.arm.exe
254361d4af8c6100d780f25a16208bb5a247005a	cia.darwin.amd64
bd8dd89c484b8c171bc6fa77ba0823eaecc59a4d	cia.windows.amd64.exe
9b14fb911d72eebc444e217bde99f2b304ba6752	cia.linux.arm64
a6390871b17b96767309644d421a83965b6031c9	cia.linux.arm
edddbf8df94d1369bc3e30dea76858dff4aa3be0	cia.darwin.arm64
61fd16cf9c6a5de02fbdb6e6d7240a00a4a62d7b	cia.linux.386
e7788b2df21a2729ee261cfcc0c2a17c7e458a61	cia.linux.amd64

URLs
tinybit[.]cc
gamecoins[.]codes
gamecodeclaim[.]com
gamesapp[.]pro
playersworld[.]xyz
lucymods[.]com
redirekt[.]in
rebrand[.]ly
gluegames[.]xyz
igetforfree[.]com
techdoy[.]com
gamemasters[.]xyz
fabgames[.]xyz
knightmods[.]com
gamehunters[.]win
getfreegem[.]com
betabuff[.]xyz
gamesconquest[.]xyz

gamersahead[.]com
gamedip[.]xyz
bizgames[.]xyz
gamedips[.]xyz
gamedips[.]com
tapasgaming[.]xyz
iwantforfree[.]com
gainforfree[.]com
bigmouse[.]club
flamingame[.]com
codesrbx[.]com
free-albums[.]org
lootcodes[.]com
madgames[.]xyz
gopremium[.]win
giftboxfree[.]com
cheersgamers[.]com
gamervalvet[.]com
gamesflow[.]xyz
nastygames[.]xyz
gameysky[.]xyz
buxx[.]site
gamerblind[.]com
gamemasters[.]xyz
gamecodeclaim[.]com
wikiredeem[.]com
codefy[.]xyz
gaminghorn[.]com
hackcheatsgenerators[.]com
coub[.]com
wbld[.]xyz
arcades[.]tech

gamerscrew[.]xyz
kaciestarrtriplett[.]com
gopremium[.]win
vipgamesgen[.]com
freerobux[.]best
rbxt[.]site
boom-beach-free-diamonds[.]com
gamecheats[.]win
dragon-city-free-gems[.]com
getfortskins[.]com
unlocker[.]cc
webstoreusa[.]net
sbld[.]xyz
newsdashes[.]com
chatgamings[.]com
m[.]vegas7games[.]com
giftcardsking[.]xyz
nancymarkle[.]com
g4ming[.]cc
justpremium[.]xyz
kachifpro[.]info
ocean-of-hacks[.]com
appmobileforce[.]com
gemtoon[.]com
cheersgamers[.]compubg
techiesbay[.]com
supergame100[.]com
vegas7games[.]pro
windmod[.]icu
gamerslab[.]org
smash[.]gg
bandicam[.]com

onergfx[.]xyz
wefunder[.]com
flamingame[.]comproject
devices[.]by
gametown[.]xyz
gainforfree[.]compubg
imv[.]quest
spotifyplus[.]pro
thenewsref[.]com
correlsense[.]com
instagramhackonline[.]com

MD5
68b09896b65db21d2c6cd2923d2486a2f69f73ef
557af28f0a42d4fb7466376ce422bcb518e7ccc0
1378d35524804d2f0e42fc1e8e6365211713731f
3859aa3ddc941be0d8459b90244f7cb0f48da1be
268546ab1aedee336151933159f056c45844ef4c
3eaa0ced4d19742c35bc3d9a99636e5333ceb573
94f6ba66169f54975771d6201bd8a40a65ffee16
9e0373a8e50a1a87a552cd25cfdad51322b00719
3c4d2e0f3125817c10ae4aa4a29a8ddcedbe3065
f8438699804645ebc7cc573cc1326050814b02e4
661450bd7934ae7a138a040d9d27b086414237d3
de2a6dfbed323e0109ce02737df1d9ce5de38561
1a891771806974ec18111a6c69b6d5bb92d6298d
a219cec2f4a3ea2c2a707925473ebe68b620e75c
596659f434ef78a4f7433c59d3efa79d50fa3de2
d932be913409595ecc1d94e644c5050f5d5ce5a3
8d02c52b03b034774bfb6767d53569035aa6398b
52bf75dc7db3db210eea58bcea31d6cf7964a5d1

1ee6eace8ccf865fc4ddb67d895833ad664f7a5b
d394756d77d2cd85fce527c3cd3c1e4c7ebdd1fb
b4a490e54f9ed0f584de48dad80cc35217fa528d
0b25161aa8a4e0ea3be8ad8870409e4c93941086
19a6b849d6bcb7a8dbbbde2158923135c0ee647c
508a81ffe18fd608fddcb73ea2aba4a83c1a8fc3
12ea7268665ea0e2688a47278c6b24ea6f907535
ed5433e5c3b836ee9a4f9f3dde6c8b4e703eca0e
9673c811de0ab875b542eaabfed121100f3ffad9
1dca0855dd4175dadbe2f9917ad4e1ab176c8052
7298b2bbf8558259ed8a5f2a286e1c2607e85bd5
3bd886c69d380745a2db2a2da3b8d9adbff4627e
c5af9a6308e4720a451f79124ee238ce8e021087
43d2dbe829300587d5672c9209c39233a0d1ff8d
37407dbd8f41a896ce8c68bc2eb5a7041e9fe47d
b3a35866f23496cf52b8c7ad609f64b39003a386
5ac10152a5db8b5f3ca827616a526314ad9b8983
3f62cd17186dd821495080b7fed822ad271b9a24
ca3aecd84b5b82ee0dac98223111bf300fec6441
2ee8cec7f388873ad50c6108e16225b344035e4c
1a16d6cacd5cd19b143d88f6f93cb15b535e8f15
9ba06781f172dd8a0bfd333c6f18ea7b15af3d85
761cfd2c1c38477ff27291b841f27c345622d58f
adc917741164cc59da629cc4fd44f9f46ec06a2d
085b0b8974a8d93998a2dafb1335306b676274eb
48fda8ccdf50e7c210c3cffe1af3572b1962bd68
e4f6c8886de708a4c16e88e3ebf17f60adfacbad
5d843c53ef47ef89a1ab4a8d2e58bb9c2ae6bf34
bc890c4578ba52a27902c4b6e2bfe0c18ca84a2d

IP
54.254[.]189.27

IP
54.254[.]189.27

Appendix 1D – Godfather Banking Trojan

Domains
henkormerise[.]com
banerrokutepera[.]com
heikenmorgan[.]com
pluscurrencyconverter[.]com

MD5
d7118d3d6bf476d046305be1e1f9b388
7e061e87f9a4c27bfb69980980270720

SHA256
c79857015dbf220111e7c5f47cf20a656741a9380cc0faecd486b517648eb199
b6249fa996cb4046bdab37bab5e3b4d43c79ea537f119040c3b3e138149897fd

Appendix 1D – Godfather Banking Trojan

SHA256
646ea89512e15fce61079d8f82302df5742e8e6e6c672a3726496281ad9bfd8a
4b6d8590a2db42eda26d017a119287698c5b0ed91dd54222893f7164e40cb508
c33e50c3be111c1401037cb42a0596a123347d5700cee8c42b2bd30cdf6b3be3
71453640ebf7cf8c640429a605ffbf56dfc91124c4a35c2ca6e5ac0223f77532
3188cbe5b60ed7c22c0ace143681b1c18f0e06658a314bdc4c7c4b8f77394729
80fba2dcc7ea2e8ded32e8f6c145cf011ceb821e57fee383c02d4c5eaf8bbe00
De85f1916d6102fcbaceb9cef988fca211a9ea74599bf5c97a92039ccf2da5f7
2a0397adb55436efa86d8569f78af0934b61f5b430fa00b49aa20a4994b73f4b

C2 and Domains
hxxp://77[.]73[.]133[.]99/taka
hxxp://77[.]73[.]133[.]99/trester
hxxp://77[.]73[.]133[.]99/pause
hxxp://77[.]73[.]133[.]99
hxxp://77[.]73[.]133[.]99/selects?dram=1
hxxp://77[.]73[.]133[.]99/selects?bilert=1
hxxp://77[.]73[.]133[.]99/route?index=1
hxxp://77[.]73[.]133[.]99/route?alert=1
hxxp://89[.]208[.]107[.]12
hxxp://89[.]208[.]107[.]12/selects?param=1
hxxp://89[.]208[.]107[.]12/selects?walert=1

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.

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com
info@payatu.io
+91 20 41207726