Payatu

February 2023

Cyber Threat Intelligence Report

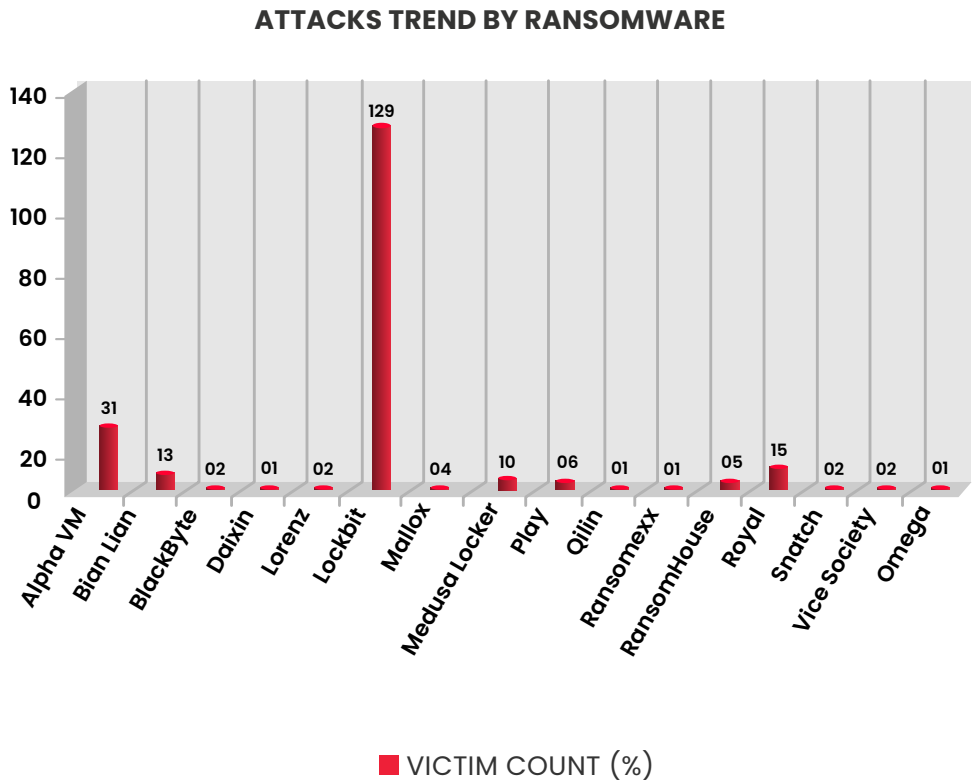
Payatu Security Consulting Pvt. Ltd.

Table of Contents

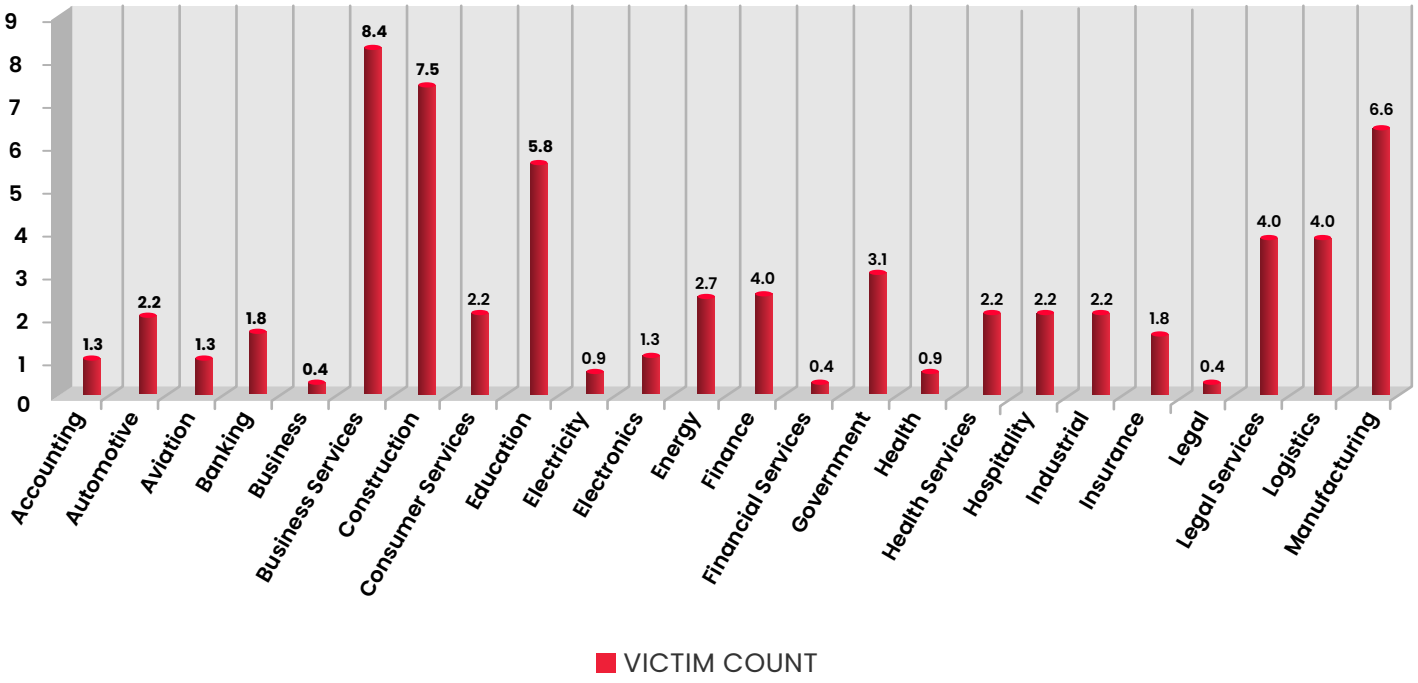
01

Ransomware Statistics

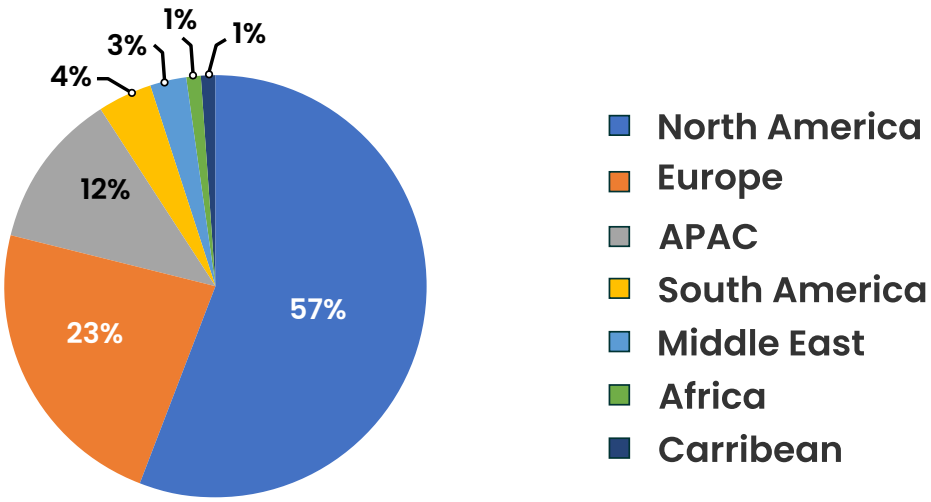
- LockBit Ransomware group claimed to have compromised Indian Chemical Conglomerate SRF Limited.
- Mallox Ransomware claimed to have compromised Indian Non-Profit Organization – FICCI.
- LockBit Ransomware claimed to have compromised US based Insurance company – DelawareLife
- AlphVM Ransomware claimed to have compromised Australian Finance organization – Smarter Capital.
- Snatch Ransomware claimed to have compromised US based Business firm MSX International.



ATTACK COUNT



REGION-WISE ATTACKS TREND



Country-wise Attacks Trend - 226

 Argentina - 2

 Australia - 8

 Belgium-2

 Bolivia - 1

 Brazil - 4

 Canada - 8

 China - 3

 France - 9

 Greece - 1

 Indonesia - 4

 Ireland - 1

 Italy - 8

 Jordan - 1

 Mali - 1

 Norway - 1

 Malaysia - 1

 Mauritius - 1

 Mexico - 3

 Netherlands - 2

 Oman - 1

 Portugal - 1

 Romania - 1

 Singapore - 2

 South Korea - 2

 Spain - 3

 Switzerland - 1

 Tonga - 1

 United Arab Emirates - 3

 United States of America - 109

 Vietnam - 2

02

Lazarus Group of North Korea Targets Healthcare Research Organizations in India

Tags: Healthcare, Defense, Energy, Research, Supply Chain, India, Lazarus Group

As per a report from WithSecure labs, Q4-2022 observed multiple attacks targeting public and private research organizations, medical research, the energy sector, and their supply chain. Referencing an error message in a backdoor, the report named "No Pineapple" discusses in detail the activities that led to its attribution to the North Korean state-sponsored APT group, the Lazarus group.

Initial compromise and privilege escalation begin with exploiting known vulnerabilities in unpatched Zimbra devices, namely, CVE-2022-27925 and CVE-2022-37042. These are compromised using webshells developed in JSP, followed by the installation of tunneling tools like Plink and 3Proxy for primary connection to endpoints. As it's a standard user access level, a privilege escalation to root is performed using CVE-2021-4034 through pwnkit.

Further tactics were executed after a connection was set up with the C&C server, from where the Grease malware was downloaded to gain admin access on lateral machines and harvest credentials. The Cobalt Strike beacon, regularly connecting to the server, was the indicator pointing to the 100GB exfiltration operation from the respective organization.

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

03

SideCopy APT Group Targets Government Entities in India

Tags: Government, India, SideCopy APT, Phishing

Recent monitoring activity performed by Threatmon.io observed spear phishing activities targeting Indian Government entities. A file named "Cyber Advisory.docm" superficially focuses on notifying its readers about Android Threats and Prevention, pretending to be sent by the Ministry of Communications (Department of Telecommunication).

The document suggests that the victim enables macros, if the victim does so, then its macros retrieve HTML content from a domain, followed by conversion from Hex content to a binary named vlan.exe, stored under the StartUp directory. The executable is a new version of ReverseRAT, a commonly used malware by SideCopy. With long sleep methods, the RAT attempts to avoid detection, followed by connecting to the C&C server. The data is sent to the C&C after encryption using RC4.

Since the target is a government entity, the aim of the group is to maintain persistence rather than data exfiltration. Hence, the RAT awaits further commands from the C&C server.

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

04

Chinese Threat Actors Launch Malicious Ad Campaigns to Target East and Southeast Asia

Tags: Fake Applications, Malicious Advertisements, East Asia, Southeast Asia

Researchers at Eset, have identified malware campaigns led by Chinese threat actors, wherein **malicious advertisements appearing on Google Search are loaded with trojanized installers.** This is done by setting up fake websites that host popular applications such as Firefox, WhatsApp, and Telegram that are injected with FatalRAT, a remote access trojan granting access to the victims' computers.

Once these applications are downloaded, the MSI installer installs legitimate installer and executes it, with parallel creation of scheduled tasks (T1053.005). The legitimate application then side-loads (T1574.002) a malicious loader. As this file is executed, the shellcode loads and runs malicious DLL library that decrypts and executes FatalRAT.

FatalRAT can capture keystrokes, terminating browser processes and stealing or deleting browser data. It can also detect virtualization and act as an intermediary for main attacks like ransomware. This can be done by its capability of downloading and executing other files. The techniques in this version have been updated from previous versions.

05

Cryptocurrency Users Targeted by MortalKombat Ransomware and Laplas Clipper Malware

Tags: Cryptocurrency, Malware Campaign, MortalKombat Ransomware, Laplas Clipper

A malware campaign targeting cryptocurrency users has been identified by Cisco Talos, wherein cryptocurrency luring emails are being used to compromise victim machines using relatively new ransomware and GO variant of the Laplas Clipper malware. The threat actor is observed to be scanning victim machines for exposed RDP ports targeting individuals, small businesses, and large organizations and demanding ransom payments.

The attack begins with phishing emails consisting malicious attachments (T1566.001) and impersonating CoinPayments, a legitimate crypto payment gateway. The attachment contains a bat loader script that uses bitsadmin (a LOLBin) to download a zip folder to the %TEMP% folder from the attacker's server. The script then proceeds by unzipping into either MortalKombat ransomware or Laplas Clipper malware in form of an executable file and parallelly deleting the ZIP files to avoid detection.

MortalKombat ransomware, which was first observed in January 2023, encrypts system files, backups, databases, remotely mapped logical drives and other critical locations. It also corrupts Windows Explorer, removes applications and folders from Startup and disables RUN command on the victim's machine.

Laplas Clipper as the name denotes, is a clipboard stealer first observed in November 2022. Specifically targeting crypto users, this malware uses regex to monitor the victim's clipboard for cryptocurrency wallet addresses.

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

06

PureCrypter targets Government Entities in APAC and North America Region

Tags: Government, APAC, North America, Malware, RAT

Active since March 2021, Purecrypter is an advanced downloader that is used to download secondary malware, like Agent Tesla. Interestingly, the payload is downloaded from a Discord server, link to which is sent via email. The email consists of a password protected zip file, with a relatively simple password.

As the folder is uncompressed, the malware is extracted and further goes on to download a secondary malware from a compromised non-profit organization. As mentioned above, downloaded malware is Agent Tesla, communicating back to an FTP server in Pakistan, sharing data like stolen passwords, screen logging, screen capturing etc. through process injection (T1055).

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

7

Appendix

Appendix 1A – Lazarus Group

Hash	Name
7c40d4ded95f425fa01895f9d4359c9ef250290a	Grease malware
9d97c6920385c20cd1023fb9f094bf35e0efbadf-33576d457834e 51c2ef1270	Plink
2963a90eb9e499258a67d8231a3124021b42e6c70dac-d3aab36 746e51e3ce37e	3Proxy
47f12a1976552a1319bd58d813f213d7ebdef4fa	Dtrack malware
46a934e7b42bfb0a2a9bcecade78f63375192924	Acres.exe [RAT]
b2b36600ce41129fa85a15a7177a61b7cb714000	Mimikatz
8c384b77b7100d6469e5e7b5cfa779dbcbcaa9ab	Webshell
88df19687e6aa8da376e37a8d71421b5b78a2cb4	Webshell
61156df8e4a5eadac8137c1cbd55145eab654726	Webshell

Network	Name
104.225.129[.]86	Cobalt Strike C2
104.225.129[.]103	Cobalt Strike C2
15.207.207[.]64	Acres.exe C2
209.95.60[.]92	
175.45.176[.]27	
23.237.32[.]34	
193.176.211[.]0/24	
146.185.26[.]150	
154.6.26[.]2	

Appendix 1B – SideCopy APT group

Hash
b277a824b2671f40298ce035686a2ccc0fca2a081a66230c57a3060c-2028f13ee
8b87459483248d7b95424cd52b7d4f3031e89c6644adc2e167556e071d9e-c3aa

Network
http[://]luckyoilpk[.]com/vlan.html
http[://]185[.]174[.]102[.]54:443

Appendix 1C – FatalRAT

Hash
00FD2783BBFA313A41A1A96F708BC1A4BB9EACBD
3DAC2A16F023F9F8C7F8C40937EE54BBA5E82F47
51D29B025A0D4C5CDC799689462FAE53765C02A3
64C60F503662EF6FF13CC60AB516D33643668449
2172812BE94BFBB5D11B43A8BF53F8D3AE323636
3620B83C0F2899B85DC0607EFDEC3643BCA2441D
1FBE34ABD5BE9826FD5798C77FADCAC170F46C07
23F8FA0E08FB771545CD842AFDE6604462C2B7E3
C9970ACED030AE08FA0EE5D9EE70A392C812FB1B
76249D1EF650FA95E73758DD334D7B51BD40A2E6
DBE21B19C484645000F4AEE558E5546880886DC0
1BE646816C8543855A96460D437CCF60ED4D31FE
B6F068F73A8F8F3F2DA1C55277E098B98F7963EC
2A8297247184C0877E75C77826B40CD2A97A18A7
ADC4EB1EDAC5A53A37CC8CC90B11824263355687
EF0BB8490AC43BF8CF7BBA86B137B0D29BEE61FA
AD4513B8349209717A351E1A18AB9FD3E35165A3

Network
107.148.35[.]6
107.148.45[.]20
107.148.45[.]32
107.148.45[.]34
107.148.45[.]37
107.148.45[.]48
193.203.214[.]75

Tactic	ID
Resource Development	T1583.001
	T1583.003
	T1585.003
	T1608.001
	T1587.002
Initial Access	T1189
Execution	T1204.002
	T1059.003
	T1106
Persistence	T1053.005
	T1547.001
Defense Evasion	T1140
	T1027.007
	T1574.002
	T1497.001
	T1027.009
	T1553.002
Collection	T1056.001
	T1119
Command and Control	T1573.001
	T1095
Exfiltration	T1020
	T1041

Appendix 1-D MortalKombat and Laplas Clipper

Hash
9a5a5d50dea40645697fabc8168cc32faf8e71ca77a2ea3f5f73d1b9a57fc7b0
26d870d277e2eca955e51a8ea77d942ebafbbf3cbf29371a04a43cfe1546db17
1bf30c5c51a3533b4f0d7d3d560df691657d62374441d772f563376b55a60818
f02512e7e2950bdf5fa0cd6fa6b097f806e1b0f6a25538d3314c793998484220
63ec10e267a71885089fe6de698d2730c5c7bc6541f-40370680b86ab4581a47d
e5f60df786e9da9850b7f01480ebffced3be396618c230fa94b5c-bc846723553

Network
http[://]193[.]169[.]255[.]78/fw-apgksdtpx4hoaujjmbvdnxpohz[.]pdf[.]zip
http[://]193[.]169[.]255[.]78/fw-cpgk2xfpx4hoaujjmbvdnxpohz[.]pdf[.]zip
144[.]76[.]136[.]153

Appendix 1-E Purecrypter

ftp[://]ftp[.]mgcpakistan[.]com/"
Username: "ddd@mgcpakistan[.]com"

Hash
be18d4fc15b51daedc3165112dad779e17389793fe0515d62bbcf00def2c3c2d
5732b89d931b84467ac9f149b2d60f3aee679a5f6472d6b4701202ab2c-d80e99
a7c006a79a6ded6b1cb39a71183123dcaaaa21ea2684a8f199f27e16fcb30e8e
5d649c5aa230376f1a08074aee91129b8031606856e9b4b-6c6d0387f35f6629d
f950d207d33507345beeb3605c4e0adfa6b274e67f59db10bd08b91c96e-8f5ad
397b94a80b17e7fbf78585532874aba349f194f84f723bd4adc79542d90efed3
7a5b8b448e7d4fa5edc94dcb66b1493adad87b62291be4ddcbd61fb-4f25346a8
efc0b3bfcec19ef704697bf0c4fd4f1cfb091dbfee9c7bf456fac02bcffcfedf
C846e7bbbc1f65452bdca87523edf0fd1a58cb-d9a45e622e29d480d8d80ac331

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