Payatu

September 2022

Cyber Threat Intelligence Report

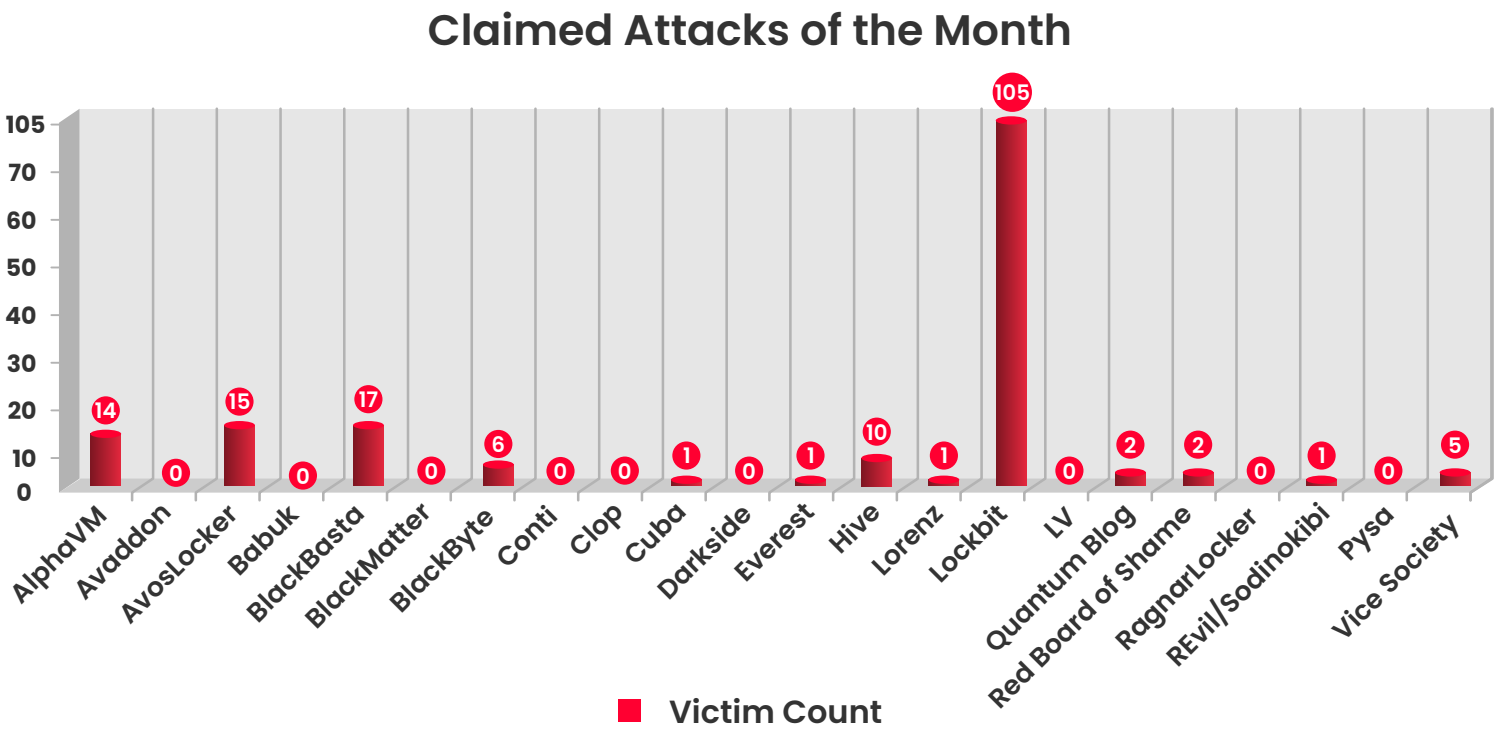
Payatu Security Consulting Pvt. Ltd.

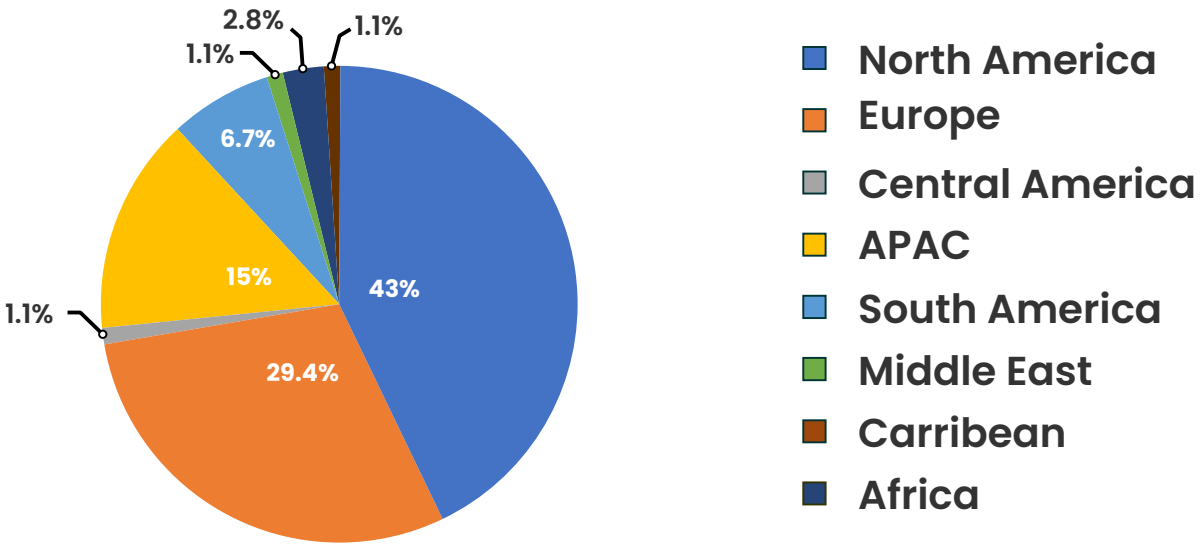
Table of Contents

01

Ransomware Statistics

- Stratford.edu claimed to be compromised by AvosLocker ransomware
- Ministry of Economia- Argentina claimed to be compromised by Everest ransomware.
- Nakamura Corp –Japan claimed to be compromised by Lockbit ransomware.
- Vice Society ransomware targets 5 educational institutions for the month of September.





Total 180
Claimed Attacks of the Month

 Argentina - 1

 Australia - 1

 Austria - 2

 Belgium - 2

 Brazil - 4

 Bulgaria - 0

 Canada - 4

 Chile - 1

 China - 2

 Colombia - 3

 Czech Republic - 1

 Costa Rica - 1

 Dominican Republic - 1

 Ecuador - 1

 Finland - 0

 France - 19

 Gabon - 1

 Germany - 6

 Greece - 0

 Hong Kong - 1

 Indonesia - 1

 Israel - 0

 Italy - 3

 Jamaica - 1

 Kenya - 1

 Luxembourg - 0

 Malaysia - 2

 Mexico - 0

 Montenegro - 0

 Morrocco - 0

 Netherlands - 2

 Nicargua - 0

 New Zealand - 2

Total 180
Claimed Attacks of the Month


Panama - 1


Paraguay - 1


Peru - 1


Philippines - 1


Portugal - 1


Qatar - 0


Seychelles - 1


Singapore - 1


South Korea - 1


Spain - 5


Switzerland - 2


Taiwan - 6


Tanzania - 1


Turkey - 2


Uganda - 1


UK - 8


USA - 77


Venezuela - 1


Vietnam - 6

02

Threat Actor Gains Access to Internal Tools of Uber, Company Claims it to be Lapsus$ Group

Tags: Uber, Lapsus$, Darkweb, Slack

On September 19th, 2022, the Uber team updated its users through an update about a security incident that occurred in their environment a few days ago. Discussing the details of the compromise, the team explained how the credentials of an EXT contractor leaked on the darkweb helped the threat actor gain access to the environment. Once gaining initial access, the threat actor then went on to access other employee accounts and some internal tools such as G-Suite and Slack.

As the image circulating over the internet shows, the threat actor had sent out companywide messages through Slack. As of now the team at Uber has been monitoring its systems, and initial investigation shows that there has been no access to its production environment, user database, or any other user information.

According to the team at Uber, the attacker belongs to the recently famous Lapsus$ group that has also been sighted in various other security incidents at technology companies like Microsoft, Cisco, Samsung, and Okta. While the investigation is ongoing, the team at Uber believes that it is highly unlikely that any major business impacts have occurred due to this breach of security.

03

After Uber, Rockstar Games also Compromised

Tags: RockStar Games, Data breach

Developing popular games like the Grand Theft Auto series, Max Payne, and many others, Rockstar Games has been one of the most successful gaming companies ever. However, in the month of September, the company came into the limelight for completely opposite reasons, wherein, through its official Twitter handle, the company disclosed being compromised and that the footage of its latest Grand Theft Auto game is leaked by being released to the public.

On September 19th, 2022, the company shared through a post on Twitter about how an unauthorized third party illegally accessed their systems and was able to collect critical information like early development footage of the Grand Theft Auto game. Though the company has not shared any information on the source code leaks, there have been claims publicly that in addition to the footage, the source code of the game has also been leaked. As of now, no group has claimed responsibility for the breach but there have been instances mentioning that the leaks were possibly done by the Lapsus$ group.

04

Emotet Now Being Used to Load BlackCat and Quantum Ransomware

Tags: Emotet, Quantum, BlackCat

Originally developed in 2014, the Emotet malware was used as a Banking Trojan, and just prior to its shutdown, it was observed to be used as a tool for initial access used by the Conti ransomware. Since its re-emergence, malware has been observed to be used as a tool for initial access used by other ransomware like Quantum and BlackCat.

With an evolving attacker flow, Emotet now works as a dropper or downloader, which downloads a Cobalt Strike beacon, and then is followed by deployment of payload that goes on to propagate through the victim's environment and execute ransomware operations. A detailed blog can be investigated at AdvIntel's website.

05

Microsoft Teams Targeted by GIFShell Attacks

Tags: Microsoft Teams, GIFShell

A researcher identified a vulnerability in Microsoft Teams, which allows an attacker to send malicious GIF files through external sources to a victim, causing the possibility of dropping malicious files that can execute remote code. The attack through crafted social engineering can send SharePoint links of a file that are not validated by the inbuilt capabilities of Teams. The impacts of this attack ranges from remote code execution to complete access to a victim's machine.

The attack starts with an unknown user outside a company domain sending out a GIF file to the victim. As the option of sharing an attachment is not present for external users, there are no validations put in place for checking such attachments. The attachment is generated as a SharePoint link to the file, which can only be viewed by the sender recipients' Teams. When the victim clicks on this link, a JSON body is sent out as a POST request including several other attributes apart from the SharePoint link.

This JSON body can be changed and a file format that Teams doesn't know, like a DLL file can replace the original one and can allow a one-click RCE via NTLM relay in Microsoft. The impact of such an attack is that the NTLM hash of the victim can be sent to an SMB listener, while forwarding it to Domain Controller, resulting in an RCE at the victim's end.

06

LastPass Breached, Hackers in the Environment for Few Days

Tags: LastPass, Data breach

On September 15th, 2022, the CEO – LastPass notified its users of a security incident that occurred at LastPass Developed Systems. Denying any compromise of customer data or encrypted vaults, the team shared details about the incident of how the attacker accessed a developer's system which had no contact with the production environment.

After a detailed analysis, it was confirmed that the production servers hosting the source code and builds had no attempts of code poisoning or malicious code injections. Such attacks are an important reminder for organizations to properly define security controls and always separate production and development environments. For a detailed disclosure, kindly refer to the blog by LastPass.

07

DPRK-Based Threat Actors Targeting Victims via WhatsApp Phishing and Malicious Putty Executable

Tags: Mandiant, Research, DPRK, Whatsapp, Putty

In an ongoing investigation, threat hunters at Mandiant have identified some new attacking vectors being used by threat actors from DPRK (Democratic People's Republic of Korea aka North Korea). The threat actors have been identified luring victims via fake job offer. The initial contact is made via an email that offers a job at Amazon.

After convincing the victim that the offer and channels are legitimate, the threat actor communicates with the victim through WhatsApp by sharing an ISO file. The ISO archive contains two files, an executable - a Putty executable and a text file - a README file containing connection details. The Putty file looks like an original file, but on closer inspection, it is observed that the file with higher entropy is a trojanized version having a C-based code. This code is triggered when the victim attempts to establish an SSH connection. Irrespective of the connection state, the code is triggered, followed by the later stages of the attack.

08

Zero-Day in WordPress Plugin Backupbuddy

Tags: WordPress, Zero-day

On September 6th, 2022, the team at Wordfence identified a zero-day in one of the WordPress plugins named Backupbuddy, which is used as a backup solution for WordPress. This vulnerability makes it possible for unauthenticated users to download arbitrary files from the affected site which may or may not include sensitive information.

The vulnerability affects versions 8.5.8 through 8.7.4.1 and has now been patched as of September 2nd, 2022. As a backup feature, it is possible to take backups and store data on Google Drive, OneDrive, and AWS. However, it is also possible to download the files to a local system via the local directory copy option, a feature within this plugin that allows triggering a function via an administrative page, including those that do not require any authentication. Since the vulnerability has been identified, the Wordfence team has blocked approximately 4.9 million attempts from attackers, most commonly trying to retrieve files like *wp-config.php and /etc/passwd.*

09

Originlogger, a Keylogger Software that Succeeds Agent Tesla

Tags: Originlogger, Palo Alto, Research, Agent Tesla, MSHTA

Researchers at Palo Alto have identified a new keylogger that has a very similar UI to Agent Tesla, due to which it has also been flagged as Agent Tesla. Agent Tesla, which is a .NET based trojan surfaced in 2014, spread across via email campaigns as a link or attachment leverages several vulnerabilities such as CVE-2017-11882 and CVE-2017-8570.

Presenting a web panel and malware builder, the malware can collect data from various sources, such as Facebook, Twitter, Gmail, Instagram, Skype, Discord, etc. Initially spread through a Microsoft Word document that included numerous Excel worksheets, each workbook contains a macro that executes a file at a particular location. Once this is downloaded, it executes mshta for contents of the file that opens a web page. This web page has a JavaScript ready to be executed and download some data from a bitbucket.

10

Fake Mobile Banking Applications Targeting Indian Banking Customers

Tags: Mobile Banking Reward Apps, Indian Banking, Trojan, SMS campaign

In a recent analysis of suspicious info-stealing malware, security experts at Microsoft Defender Research Team have identified a massive ongoing SMS campaign. The campaign targets banking reward apps and sends out links to fake websites hosting malicious downloadable applications. These applications are downloaded on the victims' phones, then compromise the devices.

After the application is downloaded and installed, it triggers events like phone reboot, changing battery status and device charging. Along with these actions, the stealer module also activates and starts collecting details like call logs, SMS (focused on OTPs), credit card details, and stores it on the device. After the device is restarted, this locally stored information is sent out to a C2(Command and Control).

The fake application detected as TrojanSpy:AndroidOS/Banker.O connects to a C2 which is related to 75 other malicious APKs based on OSINT. The continuous evolution of malware in the future might also allow attackers to steal data from other applications. The recommended actions to protect against such attacks are: downloading applications from official stores only, thinking before clicking on a URL, and always keeping the installation from unknown sources option disabled.

11

Appendix

Appendix 1A- WhatsApp Phishing

Malware Family	MD5	SHA256
ISO Attachment	90adcfdaead2fda42b9353d44f7a8ceb	8cc60b628bded497b11dbc04facc7b5d7160294cbe521764df1a9ccb219bba6b
ISO Attachment	6d1a88fefd03f20d4180414e199eb23a	e03da0530a961a784fbba93154e9258776160e1394555d0752ac787f0182d3c0
Trojanized PuTTY Dropper	8368bb5c714202b27d7c493c9c0306d7	1492fa04475b89484b5b0a02e6ba3e52544c264c294b57210404b96b65e63266
Trojanized PuTTY Dropper	18c873c498f5b90025a3c33b17031223	cf22964951352c62d553b228cf4d2d9efe1ccb51729418c45dc48801d36f69b4
Themida-Packed Dropper for DAVESHELL	c650b716f9eb0bd6b92b0784719081cd	aaad412aeb0f98c2c27bb817682f08673902a48b65213091534f96fe6f5494d9
Themida-Packed Dropper for DAVESHELL	4914bcbbe36dfa9d718d02f162de3da1	3ac82652cf969a890345db1862deff4ea8885fe72fb987904c0283a2d5e6aac4

URL
137.184.15[.]189
https://hurricanepub[.]com/include/include.php
https://turnscor[.]com/wp-includes/contacts.php
https://www.elite4print[.]com/support/support.asp

Appendix 1B - OriginLogger

Hash
cddca3371378d545e5e4c032951db0e000e2dfc901b5a5e390679adc524e7d9c

IP
23.106.223[.]46
204.16.247[.]26
31.170.160[.]61

Domains
originproducts[.]xyz
origindproducts[.]pw
originlogger[.]com

Appendix 1C - Fake Banking Apps

Indicator	Type	Description
734048bfa55f48a05326dc01295617d932954c02527b8cb0c446234e1a2ac0f7	SHA-256	icici_rewards.apk
da4e28acdadfa2924ae0001d9cfbec8c8cc8fd2480236b0da6e9bc7509c921bd	SHA-256	icici_rewards.apk
65d5dea69a514bfc17cba435eccfc3028ff64923fbc825ff8411ed69b9137070	SHA-256	icici_rewards.apk
3efd7a760a17366693a987548e799b29a3a4bdd42bfc8aa0ff45ac560a67e963	SHA-256	icici_rewards.apk (first reported by MalwareHunterTeam)
hxxps://server4554ic[.]herokuapp[.]com/	URL	C2 server

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.

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 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, multi-dimensional & 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.

More Services Offered by Payatu -

- IoT Security Testing
- AI/ML Security Audit
- DevSecOps Consulting
- Critical Infrastructure
- Trainings