Payatu

June 2023

Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

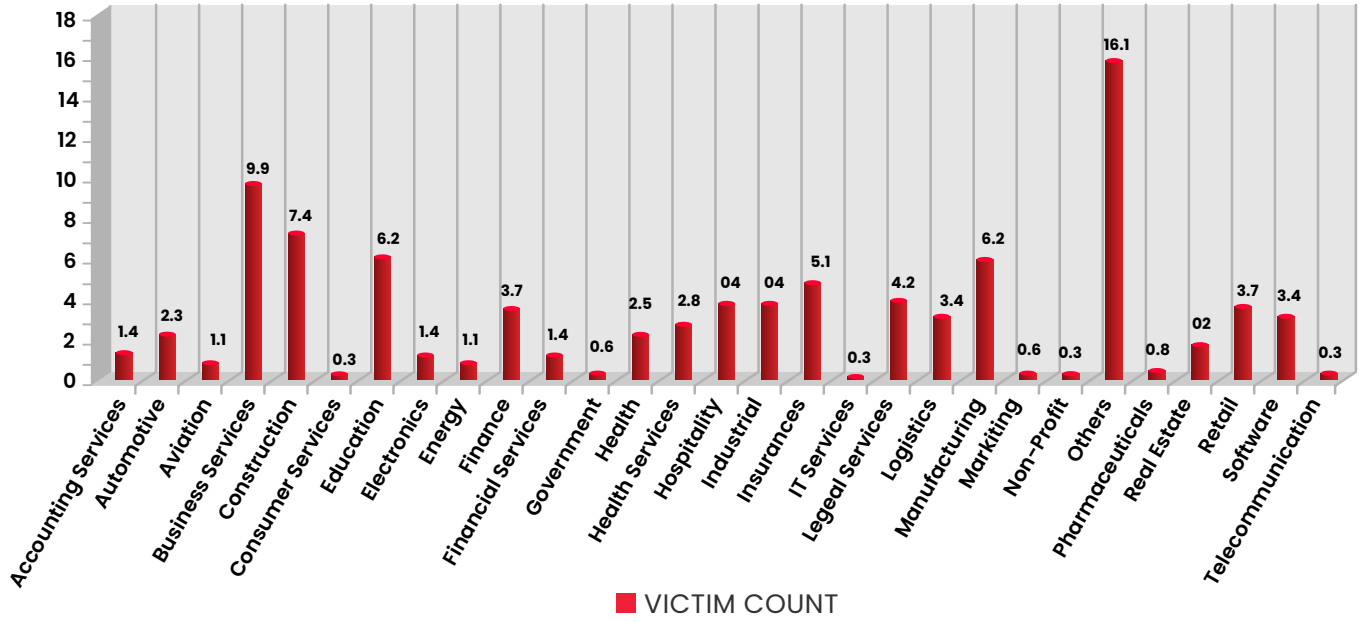
Table of Contents

01

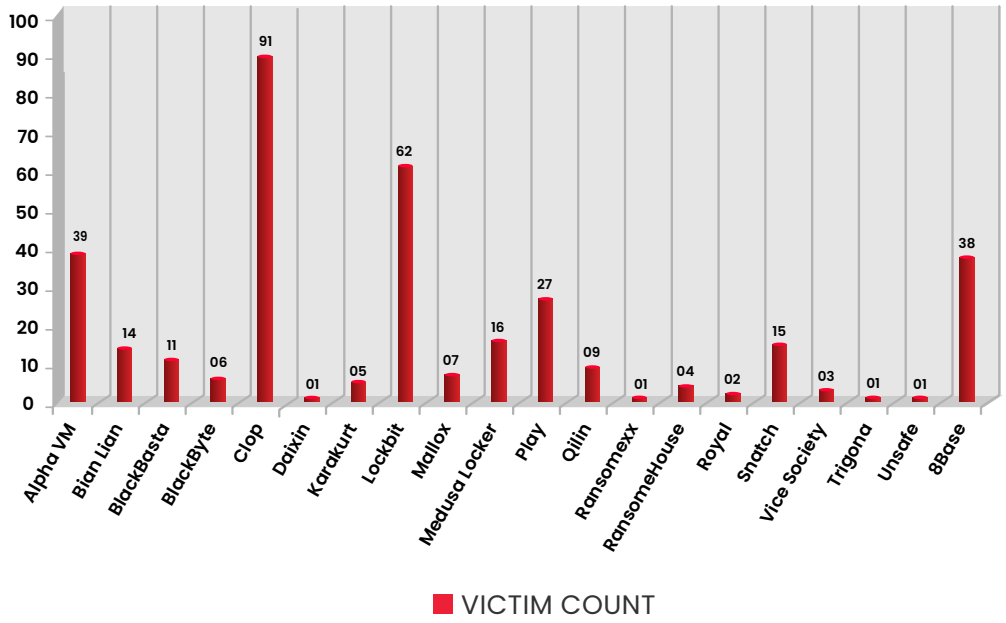
Ransomware Statistics

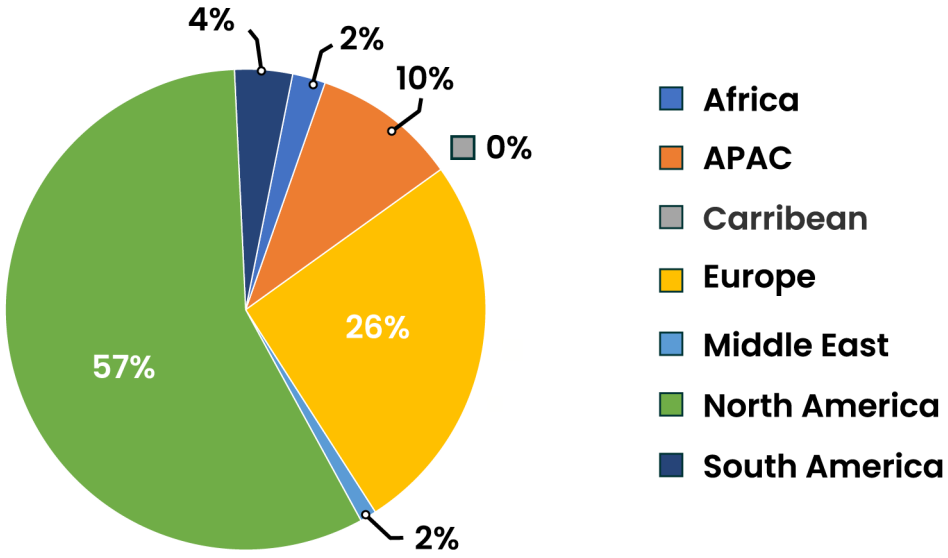
- Attributed to MOVEit vulnerability, Clop ransomware targets 91 organizations, few major players include Ernest &Young, Price Waterhouse and Coopers, Sony.
- 8base ransomware group increased the attack rate, targeting organizations worldwide, with Brazil and the USA targeted the most.

SECTOR-WISE ATTACK TREND

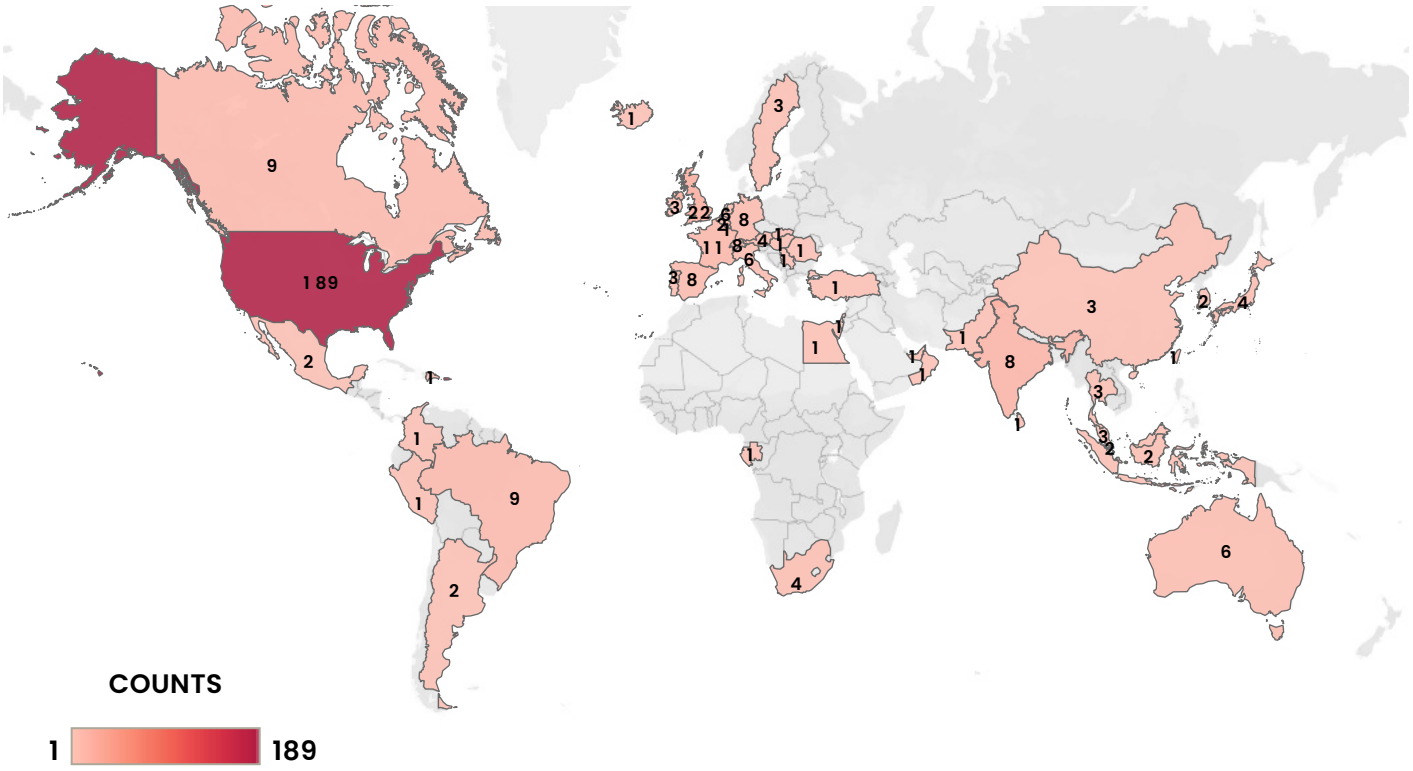


ATTACKS TREND BY RANSOMWARE





COUNTRY-WISE ATTACK TREND - 353



02

MOVEit Vulnerability Causes Global Cyber Attacks

Tags: MOVEit MFT, Clop Ransomware

MOVEit file transfer is a managed file transfer (MFT) solution used for sharing files securely with partners and customers. On 31st May 2023, a research-based organization named Forescout uncovered a zero-day vulnerability that has been actively exploited by threat actors across the globe. The vulnerability CVE-2023-34362 is an SQL Injection in MOVEit transfer software, that can result in unauthorized access, allowing privilege escalation (TA0004), and exfiltration (TA0010) of private data.

As per a CISA advisory, Clop ransomware group aka TA505, began exploiting the vulnerability a few days before it was known publicly. This exploit begins when the public facing application (T1190) of MOVEit is infected with a web shell known as LEMURLOOT that further steals data from the in-built databases. The threat group has previously been known for exploiting similar zero-days in other file transfer software.

By far, there have been more than 100 organizations that have been targeted using MOVEit vulnerability.

03

ChatGPT Credentials for Sale on Dark Web Marketplaces

Tags: ChatGPT, Artificial Intelligence

Group-IB, a cybersecurity leader based in Singapore, has recently discovered over 101,000 devices infected with info-stealing malware that contained compromised ChatGPT credentials. These findings were obtained from logs traded on illicit dark web marketplaces over the course of the last year. In May 2023, there was a significant peak of 26,802 logs containing compromised ChatGPT accounts. The rise in popularity of ChatGPT among employees, for tasks such as software development and business communications, has led to an increased risk of unauthorized access to these accounts.

ChatGPT stores user query and response history by default, potentially exposing confidential information that could be exploited for targeted attacks against individuals and companies.

The Asia-Pacific region has experienced the highest concentration of compromised ChatGPT credentials being offered for sale on the dark web. Group-IB's Threat Intelligence platform, which monitors cybercriminal forums and marketplaces, revealed that the majority of the compromised accounts were breached by the Raccoon info-stealer. Raccoon is an info-stealing malware known for collecting various types of personal data, including browser credentials, bank card details, crypto wallet information, cookies, browsing history, and device-specific information. Info-stealers, like Raccoon, aim to infect as many computers as possible to gather extensive amounts of data, which is then actively traded on dark web marketplaces.

Between June 2022 and May 2023, the Asia-Pacific region accounted for 40.5% of the ChatGPT accounts stolen by info-stealers.

04

Malware Incident Exposes Compromised NPM Package and Hijacked AWS S3 Bucket

Tags: Github, NPM, IT

As per a Checkmarx report, a recent GitHub advisory revealed a malware incident involving the NPM package "bignum". While the latest version remained uncompromised, several previous versions were affected. These versions relied on binaries hosted on an AWS S3 bucket, which was deleted six months ago, creating an opportunity for an attacker to take control of the abandoned bucket. The attacker manipulated the package's dependency on "node-gyp" to download a malicious binary file during installation.

When users installed or reinstalled the "bignum" package, they unwittingly downloaded the attacker's binary file, which appeared legitimate but included a payload to steal user credentials. The stolen data was then sent within the user-agent of a GET request to the attacker's hijacked bucket. Reverse engineering the compiled file proved challenging as it evaded malware detection.

However, further investigation uncovered suspicious behavior in the file's content and assembly code, leading to the discovery of a constructed URL and data extraction functions. This incident highlights the risks associated with compromised packages and emphasizes the need for robust security measures to detect and prevent such attacks.

05

CISA Releases Advisory on the Lockbit Ransomware with $91 Million Losses Attributed to the Group

Tags: CISA, Lockbit, Ransomware

LockBit, a prominent Ransomware-as-a-Service (RaaS) group, has caused significant damage worldwide, with approximately 1,700 reported attacks and losses totaling around $91 million since its emergence in the United States on January 5, 2020. In Australia, LockBit 3.0 was first documented in early August 2022. The French National Cybersecurity Agency (ANSSI) has encountered 80 alerts related to the LockBit ransomware since July 2020, representing 11% of all handled ransomware cases. ANSSI has confirmed and dealt with 69 incidents associated with LockBit ransomware to date.

LockBit's success lies in its innovative tactics, user-friendly administrative panel, and assurance of payment to affiliates. By employing a double extortion strategy and repurposing legitimate tools like PowerShell and batch scripts, LockBit continues to pose a significant threat. These statistics underscore the urgent need for robust cybersecurity measures to combat the evolving menace of LockBit ransomware.

06

Millions of GitHub Repositories at Risk of Code Execution Through RepoJacking

Tags: Github

Millions of GitHub repositories are at risk of RepoJacking, according to a research conducted by Aqua Nautilus. RepoJacking can lead to code execution within organizations' internal or customer environments. The study identified various popular targets, including organizations like Google and Lyft, who were promptly notified and mitigated the vulnerability. The research explores how attackers can exploit this vulnerability at scale and provides a proof of concept (PoC) based on popular repositories. Although there are restrictions on accessing old repository names (retired names), recent findings reveal numerous bypasses, rendering these restrictions ineffective.

Organizations should not rely on retired names as a security measure. In the research, a vulnerable repository is defined as the one that gets redirected, and the organization name no longer exists. Analysis of a data sample from June 2019 revealed that out of 1.25 million repositories checked, 36,983 were vulnerable to RepoJacking, indicating a success rate of 2.95%. Extrapolating this finding to GitHub's entire repository base of over 300 million repositories suggests the existence of potentially millions of vulnerable repositories.

07

MULTISTORM: Python-based Loader Malware Delivers Warzone RAT Infections via Phishing Campaign

Tags: India, USA

The Securonix Threat Research Team has uncovered the MULTISTORM phishing campaign, which employs Python-based loader malware to distribute Warzone RAT infections. This campaign predominantly targets victims in the United States and India.

The attack commences when users click on a heavily obfuscated JavaScript file within a password-protected ZIP archive. The loader malware, written in Python and packed using PyInstaller, utilizes sophisticated techniques to establish persistence and evade detection before delivering the RAT payloads. Although like DBatLoader, this Python-based loader stands out due to its unique characteristics.

Once the ZIP file is extracted, victims are presented with a single JScript file named REQUEST.js, without any obfuscation attempts. In the early stages, the loader malware employs Microsoft OneDrive links to stage various payloads. Notably, the RAT connection payloads take an interesting turn, connecting directly to an IP:Port combination with a fake [.]ddns[.]net URL appended, potentially aimed at evading network intrusion detection systems.

The MULTISTORM campaign highlights the increasing sophistication of phishing attacks and emphasizes the importance of robust security measures to counter such threats effectively.

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

08

Android GravityRAT Spyware Disguised as BingeChat and Chatico Messaging Apps Targets Indian Customers

Tags: India, Android

ESET researchers have discovered an updated version of the Android GravityRAT spyware, which is being distributed through messaging apps called BingeChat and Chatico. GravityRAT, a remote access tool used in targeted attacks against India since 2015, has now evolved with new capabilities. The BingeChat campaign, active since August 2022, is ongoing, while the Chatico campaign is no longer active.

BingeChat is distributed through a website that advertises free messaging service. Notably, this new version of GravityRAT can exfiltrate WhatsApp backups and receive commands to delete files. The malicious apps also provide legitimate chat functionality using the open-source OMEMO Instant Messenger app. ESET telemetry data suggests that the BingeChat campaign is likely narrowly targeted, as no victims have been recorded thus far.

However, there was one detection of another Android GravityRAT sample in India in June 2022. The group responsible for this malware, known as SpaceCobra internally, remains unknown, although Facebook researchers and Cisco Talos have linked GravityRAT to a group based in Pakistan.

The similarities between the BingeChat campaign and previous GravityRAT variants confirm that the malicious code in BingeChat belongs to the GravityRAT malware family. This discovery highlights the ongoing threat posed by Android spyware and underscores the importance of robust security measures to protect against such sophisticated attacks.

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

09

NSA Updates on BlackLotus Malware

Tags: BlackLotus, NSA, USA

The National Security Agency (NSA) has acknowledged the significant confusion surrounding the threat posed by BlackLotus. While some organizations describe it as “unstoppable” and “unkillable,” others believe that patches released by Microsoft mitigate the threat. The reality lies between these extremes.

BlackLotus shares similarities with Boot Hole (CVE-2020-10713) but targets Windows boot loaders instead of Linux. By exploiting a flaw in older boot loaders, BlackLotus compromises endpoint security by bypassing Secure Boot enforcement through Baton Drop (CVE-2022-21894).

The vulnerable boot loaders have not been added to the Secure Boot DBX revocation list, allowing attackers to substitute fully patched versions with vulnerable ones to execute BlackLotus. The NSA recommends system administrators within the Department of Defense (DoD) and other networks to take action.

Mitigation measures include updating recovery media, activating optional mitigations, hardening defensive policies, monitoring device integrity measurements, and being vigilant for BlackLotus variants affecting popular Linux distributions. The NSA cautions that relying solely on published patches may provide a false sense of security, emphasizing the need for ongoing vigilance and proactive defense against this threat.

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

10

Muddled Libra: A Methodical Adversary Targeting Software Automation and Cryptocurrency Institutions

Tags: BPO, IT

Muddled Libra is a threat group that poses a substantial threat to organizations in the software automation, BPO, telecommunications, and technology industries. Unit 42 researchers have investigated several incidents attributed to Muddled Libra, with a focus on large outsourcing firms serving high-value cryptocurrency institutions and individuals.

Thwarting Muddled Libra requires a combination of tight security controls, security awareness training, and vigilant monitoring. The group utilizes the 0ktapus phishing kit, which simplifies the establishment of a complex infrastructure for phishing attacks.

With prebuilt templates and a built-in C2 channel via Telegram, Muddled Libra achieves a high success rate at a relatively low cost. They employ an extensive attack toolkit, including social engineering, smishing attacks, penetration testing, and forensics tools, giving them an advantage over cyber defense measures. The group also demonstrates a strong understanding of modern incident response frameworks, making them difficult to eradicate once established.

Defenders must adopt cutting-edge technology, comprehensive security hygiene, and diligent monitoring to mitigate the risk of data loss. Modernizing information security programs is crucial in the face of Muddled Libra's high-stakes attacks.

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

11

Appendix

Appendix 1A – MULTISTORM

File Name	SHA256 (IoC)
REQUEST.zip	8674817912be90a09c5a0840cd2dff-2606027fe8843eb868929fc33935f5511e
REQUEST.js	3783acc6600b0555dec5ee8d3cc4d59e07b5078d-d33082c5da279a240e7c0e79
news.exe	18C876A24913EE8FC89A146EC6A6350CDC4F081AC-93C0477FF8FC054CC507B75
files.pdf	31960A45B069D62E951729E519E14DE9D7AF29CB4BB-4FB8FEAD627174A07B425
netutils.dll	02212f763b2d19e96651613d88338c933ddfd18be4c-b7e721b2fb57f55887d64
check.bat	5A11C5641C476891AA30E7ECFA57C2639F6827D-8640061F73E9AFEC0ADBBD7D2
easinvoker.exe	30951DB8BFC21640645AA9144CFEAA294BB-7C6980EF236D28552B6F4F3F92A96
KDECO.bat	37C59C8398279916CFCE45F8C5E3431058248F5E-3BEF4D9F5C0F44A7D564F82E
Exec.lnk	F9130B4FC7052138A0E4DBAAEC385EF5FAE57522B5D-61CB887B0327965CCC02A
Storm.lnk	0E799B2F64CD9D10A4DFED1109394AC7B4CCC317A-3C17A95D4B3565943213257
OneDrive Update.url	455ED920D79F9270E8E236F14B13ED-4E8DB8DD493D4DABB05756C867547D8BC7
OneDrive.url	9C14375FBBCE08BCF3DC7F2F1100316B2FB-745FA2C510F5503E07DB57499BFC8
storm.exe	B452A2BA481E881D10A9741A452A3F092DFB87BA42D-530484D7C3B475E04DA11
S.exe	AB0212F8790678E3F76ED90FBA5A455AC23FBB-935CF99CABC2515A1D7277676F
quas.exe	4A834B03E7FAFFEF929A2932D8E5A1839190DF4D-5282CEF35DA4019FE84B19A5
euyjrxpgo6ua.bat	11408368F4C25509C24017B9B68B19CE5278681F6F-12CE7DB992D3C6124B0A23

Appendix 1B – GravityRAT

Hash
2B448233E6C9C4594E385E799CEA9EE8C06923BD
25715A41250D4B9933E3599881CE020DE7FA6DC3
1E03CD512CD75DE896E034289CB2F5A529E4D344

IP
75.2.37[.]224
104.21.12[.]211
104.21.24[.]109
104.21.41[.]147
172.67.196[.]90
172.67.203[.]168

Appendix 1C – BlackLotus

UEFI Secure Boot DBX Hashes
B22A7B3CEBB32C80C36EAABB6F77D164AE8B76BF161F423B6E2FBF9DCB-C96C02
D355041DFBA41F8AE2CE6766ECBC88C93A743FC74F95E7E7AA3EF-32CA6E4B390
D9F629F6D1D83AC7A15DCB1116E4B9BF128758EC2EA389AA1E0DA3B8F2951150
53FCE58746C4B042B101B8682B4E52CE8B620D-3C68F69034996E33D3DDDCA1FF
F7357DD5000E1FBADBF17CC6025243A243D1BFA705801051119277A30D717B71
39C6475B3F00D92EEC049D8F6EFA010CB06F1240ED1CE7E40611278C73817471
2E094D21DC457CC4826FCD48395B92DC782F978EEF8210E4B-6F5E708527907FF
BFE0E68889A750E699788C11F08AFAE940770ED83C1B4A5DB27E10933B-29CAD1

Appendix 1D – Muddled Libra

IP
104.247.82[.]11
105.101.56[.]49
105.158.12[.]236
134.209.48[.]68
137.220.61[.]53
138.68.27[.]0
146.190.44[.]66
149.28.125[.]96
157.245.4[.]113
159.223.208[.]47
159.223.238[.]0
162.19.135[.]215
164.92.234[.]104
165.22.201[.]77
167.99.221[.]10
172.96.11[.]245
185.56.80[.]28
188.166.92[.]55
193.149.129[.]177
207.148.0[.]54
213.226.123[.]104

IP
35.175.153[.]217
45.156.85[.]140
45.32.221[.]250
64.227.30[.]114
79.137.196[.]160
92.99.114[.]231

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.