Payatu

December 2023

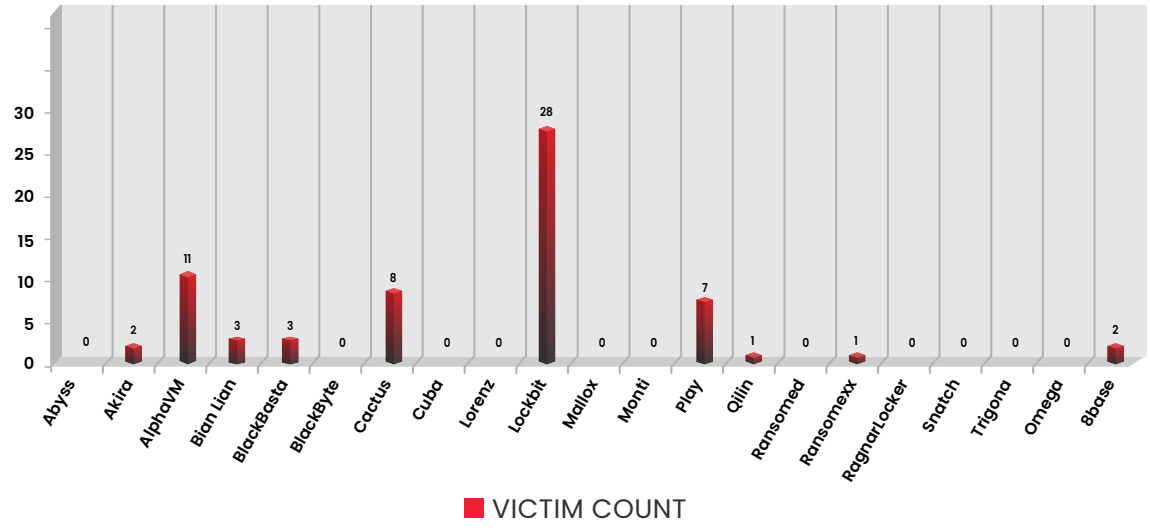
Cyber Threat Intelligence Report

Table of Contents

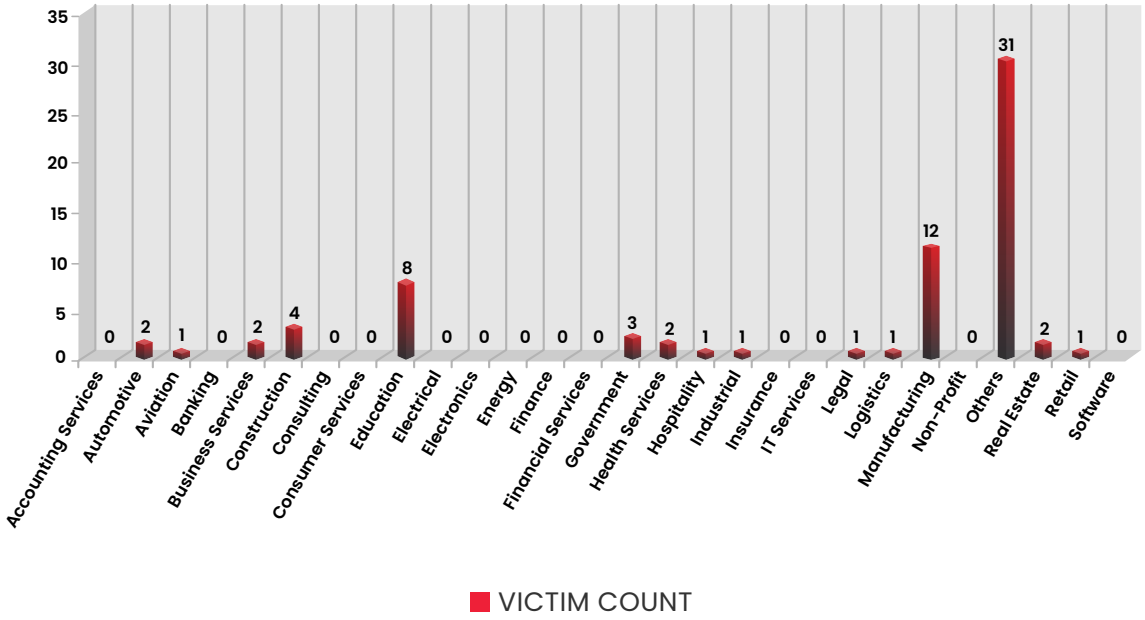
01

Ransomware Statistics

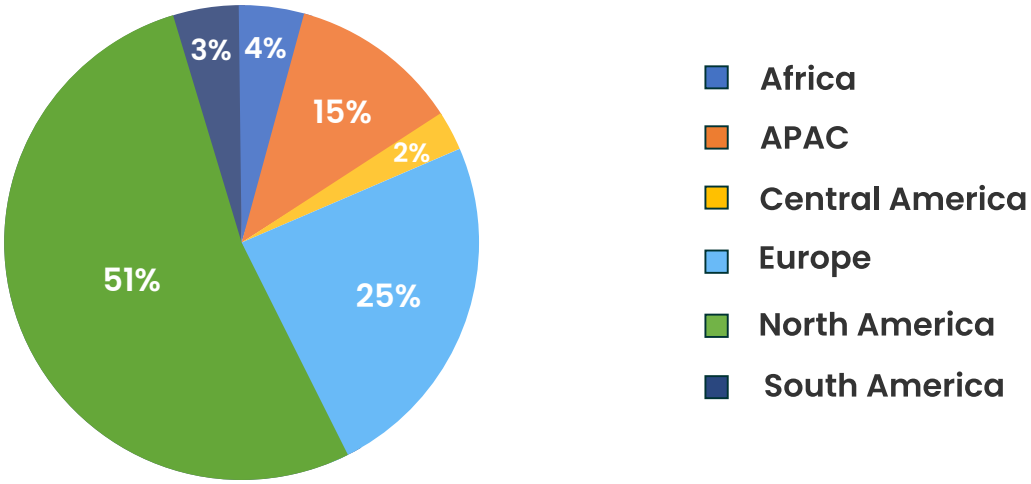
ATTACKS TREND BY RANSOMWARE



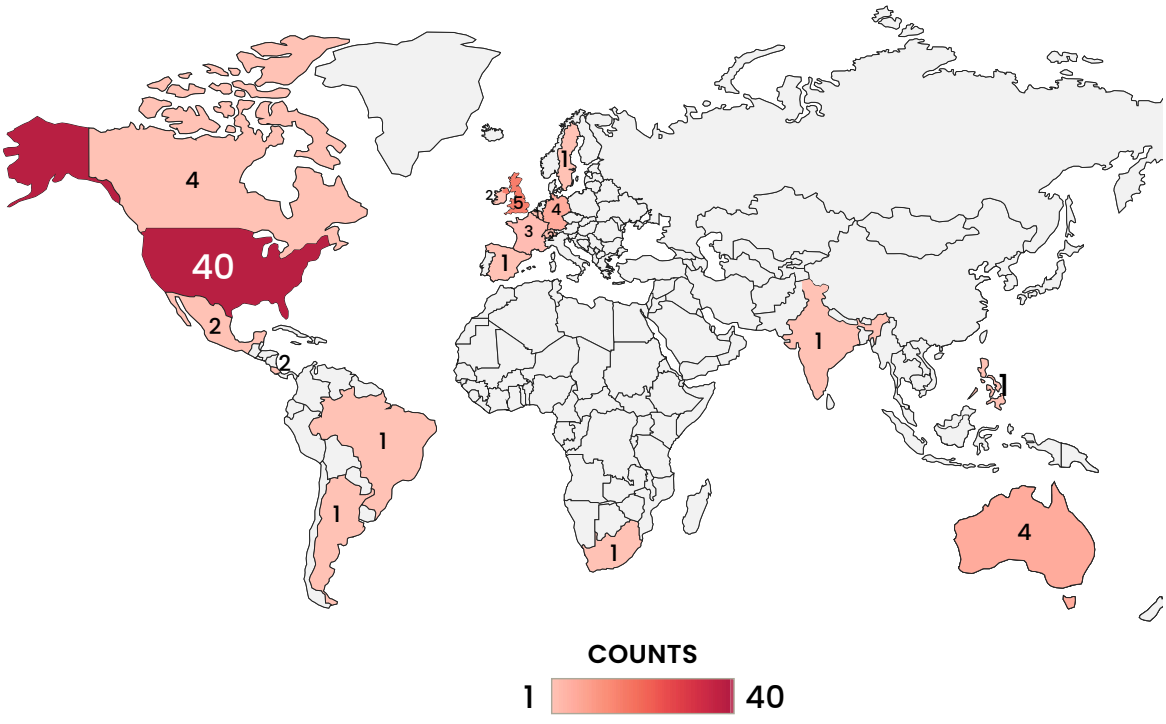
SECTOR-WISE ATTACK TREND



REGION-WISE ATTACK



COUNTRY-WISE ATTACK TREND - 75



02

Indian ISP Provider Hathway Data Breach: Hacker Leaks 4 Million Users KYC Details

Source : Hack Read
Tags: Breach Forums

A hacker operating under the alias 'dawnofdevil' has recently leaked a database, associated with Hathway, a leading Indian Internet Service Provider (ISP) and cable television service operator.

In their post on the notorious Breach Forums, where the database was leaked, the hacker disclosed that the data breach took place in December 2023 after they managed to breach Hathway's defences by exploiting a security vulnerability present in the Laravel framework application, the Content Management System (CMS) used by the company.

The hacker has shared two links, first one contains 12GB of user data, while the second link contains a staggering 214GB of information distributed across over 800 CSV files and production data. It's important to highlight that, according to the hacker, the 12GB file includes personal details of more than 41 million Hathway customers. This comprehensive data contains their full names, email addresses, phone numbers, home addresses, customer registration forms, copies of Adhaar cards with the forms, and other personal information including KYC data.

03

Iran's 'Peach Sandstorm' Cyber Attackers Target Global Defence Network

Source: Dark Reading
Tags: Peach Sandstorm

Microsoft has observed that the Iranian nation-state cyber attackers known as Peach Sandstorm is attempting to deliver a backdoor to individuals working for organizations in the military-industrial sector.

In a series of messages on X, formerly Twitter, Microsoft Threat Intelligence said that the Peach Sandstorm advanced persistent threat (aka APT33, Elfin, Holmium, or Refined Kitten) has been attempting to deliver the FalseFont backdoor to various organizations within the global infrastructure that enables the research and development of military weapons, systems, subsystems, and components.

Microsoft Threat Intelligence says FalseFont is a custom backdoor with a "wide range of functionalities" that allow operators to remotely access an infected system, launch additional files, and send information to its command and control servers. FalseFont was first observed being used against targets in early November 2023. It was not clear if there were any detections of successful infections.

Microsoft said that Peach Sandstorm has consistently demonstrated interest in organizations in the satellite and defence sectors in 2023. The development and use of FalseFont is consistent with the Peach Sandstorm activity observed by Microsoft over the past year, suggesting that the group is continuing to improve its tradecraft.

04

Hamas Cyber Attackers Use 'Pierogi' Malware at Multiple Mideast Targets

Source: Sentinel Labs
Tags: Gaza Cybergang

A group of pro-Hamas attackers known as the Gaza Cybergang is using a new variation of the Pierogi++ backdoor malware to launch attacks on Palestinian and Israeli targets. According to research from Sentinel Labs, the backdoor is based on the C++ programming language and has been used in campaigns between 2022 and 2023. The attackers have also been using the Micropsia malware in recent hacking campaigns across the Middle East.

Gaza Cybergang operations over 2022 and 2023 reveal a sustained focus on targeting Palestinian entities. The discovery of the Pierogi++ backdoor shows that the group continues to evolve and supplement its staple malware arsenal, including transforming older implementations into new tooling.

The hackers distributed the Pierogi++ malware using archive files and malicious MS Office documents that discussed Palestinian topics in both English and Arabic. These contained Windows artifacts such as scheduled tasks and utility applications, which included malware-ridden macros designed to spread the Pierogi++ backdoor. Many of the documents used political themes for luring its victims and executing the Pierogi++ backdoor, such as: "The situation of Palestinian refugees in Syria, refugees in Syria" and "The Ministry of State for Wall and Settlement Affairs established by the Palestinian government."

Researchers said that Pierogi++ is proof that Gaza Cybergang is shoring up the "maintenance and innovation" of its malware in a bid to "enhance its capabilities and evade detection based on known malware characteristics."

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

05

HTC Global Services Confirms Cyberattack After Data Leaked Online

Source: Bleeping Computers

IT services and business consulting company HTC Global Services has confirmed that it suffered a cyberattack after the ALPHV ransomware gang began leaking screenshots of stolen data. HTC Global Services, established in 1990 and headquartered in Troy, Michigan is a provider of information technology, business process, healthcare, automotive, manufacturing, and financial industries services. HTC verified the attack on X but hasn't added any comment to its company website.

"Our team has been actively investigating and addressing the situation to ensure the security and integrity of user data. We've enlisted cybersecurity experts and are working to resolve it. Your trust is our priority." This announcement comes after the ALPHV (BlackCat) ransomware gang listed HTC on its data leak site, along with screenshots of allegedly stolen data.

The leaked data includes passports, contact lists, emails, and confidential documents stolen during the attack. As of now there are no IOCs released by HTC regarding this attack. But it is evident that ALPHV ransomware gang being involved in this particular attack.

Geo-politics and APTs: Geopolitical developments continue to influence APT evolutions, with cyber-espionage remaining the primary APT campaign objective.

06

‘NKAbuse’ Malware Uses Blockchain to Hide and Spread on Linux, IoT Machines

Source: Dark Reading

A sophisticated and versatile malware called NKAbuse has been discovered operating as both, a flooder and a backdoor, targeting Linux desktops in Colombia, Mexico, and Vietnam. Kaspersky’s Global Emergency Response Team (GERT) has discovered a new multiplatform malware threat that uses innovative tactics to hijack victims. The malware, dubbed NKAbuse, uses New Kind of Network (NKN) technology, a blockchain-powered peer-to-peer network protocol to spread its infection.

Lisandro Ubiedo, a security researcher at Kaspersky, explains that what makes this malware unique is the use of the NKN technology to receive and send data from and to its peers, and its use of Go to generate different architectures, which could infect different types of systems. It functions as a backdoor to grant unauthorized access, with most of its commands centring on persistence, command execution, and information gathering. The malware can, for instance, capture screenshots by identifying display bounds, convert them to PNG, and transmit them to the bot master, according to Kaspersky’s malware analysis of NKAbuse.

NKN is an open-source protocol that allows peer-to-peer data exchange over a public blockchain with over 60,000 active nodes. It aims to provide a decentralized alternative to client-to-server methods while preserving speed and privacy. At the same time, they can act as a flood and launch a devastating distributed denial of service (DDoS) attack that disrupts targeted servers and networks, potentially causing significant disruption to business operations.

This is a powerful Linux implant with flooder and backdoor capabilities that allows it to simultaneously attack targets via multiple protocols such as HTTP, DNS, and TCP, allowing attackers to take control of the system and extract information from it. The implant also includes a “Heartbeat” structure for regular communication with the bot master, storing data on the infected host like PID, IP address, memory, and configuration.

07

CISA: A Critical Flaw in Microsoft SharePoint is Now Being Actively Exploited

Source: Bleeping Computers

CISA warns that attackers are currently exploiting a critical privilege escalation vulnerability in Microsoft SharePoint that may be related to another critical remote code execution flaw. Tracked as CVE-2023-29357, the security flaw enables remote attackers to get admin privileges on unpatched servers by circumventing authentication using spoofed JWT auth tokens.

"An attacker with access to a forged JWT authentication token could use it to conduct network attacks that bypass authentication and grant access to the authenticated user's privileges", Microsoft explains. If this vulnerability was properly exploited, an attacker may obtain administrator rights. Neither the attacker nor the user require any special rights or actions.

Remote attackers can also execute arbitrary code on compromised SharePoint servers via command injection when chaining this flaw with the CVE-2023-24955 SharePoint Server remote code execution vulnerability. This exploit is not a complete exploit of the chain demonstrated by Pwn2Own and therefore does not allow remote code execution on the target system, but the attackers themselves have implemented this exploit in RCE's CVE-2023-24955 bug.

Although CISA has not yet disclosed further information regarding the active exploitation of CVE-2023-29357, it has added the weakness to its list of known exploited vulnerabilities and mandated that U.S. federal agencies fix it by the end of the month.

08

Researchers Reveal the Secret Connection Between Sandman APT and the China-Based KEYPLUG Backdoor

Source: Sentinel Labs
Tags: Sandman and KEYPLUG

Tactical and targeting overlaps have been discovered between the enigmatic Advanced Persistent Threat (APT) called Sandman and a China-based threat cluster that's known to use a backdoor referred to as KEYPLUG. It was discovered that the KEYPLUG backdoor and the LuaDream virus, which is based on Lua, co-existed in the same victim surroundings. The assessment comes jointly from SentinelLabs, PwC, and the Microsoft Threat Intelligence team based on the fact that the adversary's Lua-based malware LuaDream and KEYPLUG have been determined to cohabit in the same victim networks.

Sandman and STORM-0866/Red Dev 40 share infrastructure controls and management practices, including hosting provider choices and domain naming practices. The implementation of LuaDream and KEYPLUG reveals indicators of shared development practices and overlaps in functionalities and design, suggesting shared functional requirements by their operators.

One notable overlap is a pair of LuaDream C2 domains called "dan.det-ploshadka[.]com" and "ssl.e-novauto[.]com" which is also deployed as a KEYPLUG C2 server and associated with Storm-0866.

The commonality between LuaDream and KEYPLUG is that both the implants have similar high-level execution flows, and support QUIC and WebSocket protocols for C2 communications, with the order in which they evaluate the configured protocol among HTTP, TCP, WebSocket, and QUIC being the same: HTTP, TCP, WebSocket, and QUIC.

SentinelLabs and Microsoft discovered Sandman's LuaDream and KEYPLUG implants existing in the same victim environments, some on the same endpoints. LuaDream is a preserved module backdoor based on LuaJIT, with

version 11.0.2.1.23.1 detected in March 2023 and version 12.0.2.5.23.29 in August 2023. In one case, the KEYPLUG malware was launched about 3 months before Luay2020.). LuaDream and KEYPLUG were active simultaneously for about 2 weeks until both threats were patched. During this time, we observed no attempts to challenge or dismantle the LuaDream or KEYPLUG operators.

09

Appendix

APPENDIX 1A – HAMAS CYBER ATTACKERS USE 'PIEROGI' MALWARE AT MULTIPLE MIDEAST TARGETS

SHA1	20c10d0eff2ef68b637e22472f14d87a40c3c0bd(Pierogi Backdoor)
SHA1	42cb16fc35cfc30995e5c6a63e32e2f9522c2a77(Pierogi++)
SHA1	5128d0af7d700241f227dd3f546b4af0ee420bbc(Pierogi++)
SHA1	599cf23db2f4d3aa3e19d28c40b3605772582cae (Pierogi Backdoor)
SHA1	75a63321938463b8416d500b34a73ce543a9d54d(Pierogi++)
SHA256	32d9d85b2105392eeb6109b27eb58c7a0ea84e7804fc19cba63fffa69d63daa4
SHA256	6ce76a00f9be1d45e83e060f5546ff8aeee0201229d6b40576f575fa5ead639a
SHA256	50a237351a247529e38aaf4d0d12a6633cf66206683ac2ba4e6333a02b3961eb
SHA1	003bb055758a7d687f12b65fc802bac07368335e(Micropsia Malware Family)
SHA1	c3038d7b01813b365fd9c5fd98cd67053ed22371(Micropsia Malware Family)
SHA256	af87a91c71b3cca1184b4b1250cacec041430264d0f8ac56bde3a6b1173e84a2(Micropsia Malware Family)
MD5	b7c930c88d6c5fb36595217244110841
Domain	aracaravan[.]com escanor[.]live beatricewarner[.]com bruce-ess[.]com izocraft[.]com

APPENDIX 1B - RESEARCHERS REVEAL THE SECRET CONNECTION BETWEEN SANDMAN APT AND THE CHINA-BASED KEYPLUG BACKDOOR

Domains	dan.det-ploshadka[.]com (KEYPLUG) mode.encagil[.]com (LuaDream) ssl.articella[.]com (Suspected KEYPLUG or LuaDream) ssl.e-novauto[.]com (KEYPLUG) ssl.explorecell[.]com (LuaDream)
IP Addresses	146.70.157.20 (KEYPLUG) 172.67.216.63 (KEYPLUG) 185.51.134.27 (KEYPLUG or LuaDream) 45.80.148.151 (LuaDream)

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.