Payatu

July 2022

Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

Table of Contents

01

Hive Ransomware Upgrades its Arsenal with Malware Written in Rust

Tags: Hive Ransomware, IOCs (Indicators of Compromise), Rust, RaaS

With an increase in the number of ransomware attacks, there has also been an expansion of the RaaS (Ransomware as a Service) ecosystem. One such ransomware that is frequently used is Hive ransomware.

First observed in June 2021, the ransomware used Golang for developing its payloads and has been observed to switch to Rust, mainly for its advantages over other programming languages, such as user-friendly syntax, ability to enable fast and safe file encryption, a good collection of cryptographic libraries and complexity while reverse engineering.

In addition to switching languages, the new variant also has some other changes like String Encryption, switching cryptography mechanisms to ECDH (Elliptic-Curve Diffie Hellman) with authentic encryption with ChaCha20 symmetric cipher.

Recommending its customers to investigate IOCs in their environment, MSTIC shares some other useful insights that can be referred to in their blog.

For IOCs of the new variant, refer to Appendix 1A.

02

High Severity OpenSSL Vulnerability Causes Memory Corruption

Tags: OpenSSL, Advisory, Vulnerability, CVE-2022-2274

Addressing its users through an advisory for high severity bug, now referred to as CVE- 2022-2274, the team maintaining OpenSSL informed its users about a Heap memory corruption issue pertaining specifically to systems supporting AVX512IFMA instructions of the x86_64 architecture. OpenSSL release 3.0.4 on June 21, 2022, introduced this bug in RSA implementation, making implementation with 2048-bit private keys incorrect and leading to memory corruption during computation.

This issue allows an attacker to trigger a Remote Code Execution on the machine doing the computations and is patched in OpenSSL 3.0.5 version, while versions 1.1.1 and 1.0.2 are not affected by the same.

For any further details, refer to OpenSSL's advisory, and for clarity on the vulnerability, refer to the NIST database.

03

North Korean Threat Actors Use Maui Ransomware to Target Healthcare Industry

Tags: Maui Ransomware, State-sponsored, North Korea, Healthcare

Active since May 2021, Maui ransomware is now on the radar of CISA (Cybersecurity & Infrastructure Security Agency), for targeting industries in Healthcare and Public Health sectors. On July 06, 2022, CISA published a joint advisory on their website along with the FBI and Department of Treasury, US.

Sharing technical details about the ransomware, used by North Korean state-sponsored cyber threat actors, the agency updated ransomware TTPs and IOCs of the ransomware that has encrypted servers of electronic health record services, diagnostic services, imaging services, and intranet services. The ransomware uses RSA, AES, and XOR encryptions to encrypt target files, creating temporary copies of these files to stage output from encryption.

For IOCs related to Maui ransomware, kindly refer to Appendix 1B.

04

CISA Advisory on MedusaLocker

Tags: Financial Services, #StopRansomware, MedusaLocker, RaaS

The CISA, the FBI, and the FinCEN (Financial Crimes Enforcement Network), jointly released an advisory to share an update about the MedusaLocker ransomware, known to be targeting vulnerabilities in Remote Desktop Protocol (RDP) to gain access to victim networks. Another technique frequently used is email campaigns and phishing.

This is followed by execution of a batch script, initiating PowerShell script PEInjection, followed by propagation techniques like detecting attached host via ICMP and SMB Protocol. Encryptions used by this locker include AES and RSA-2048 and executes scheduled tasks to run the ransomware every 15 minutes.

For IOCs related to MedusaLocker, refer to Appendix 1C.

05

Cleartrip Compromised, Data Shared on a Private Forum

Tags: Data Breach, Data Leak

Cleartrip, an Indian flight booking site informed its customer via mail on July 18, 2022, about a security anomaly in its internal systems, due to illegal and unauthorized access, and has initiated protocols for such cyber incidents, which include, informing concerned authorities like CERT-IN, followed by an established procedure of cyber forensic investigation.

While the Flipkart subsidiary didn't share any further details yet, some security researchers identified threat actors selling data on a private forum, which included screenshots of data available, including a very recent B2C customer list for 2021-22, a compressed folder named Cleartrip finance and many other files. Any further reports from the company are awaited, as the same will be shared post forensic investigations.

For further information on leaked data, refer to this tweet from security researcher Sunny Nehra.

06

Pakistan-Based Threat Actor Targets Educational Institutions

Tags: Transparent Tribe, CrimsonRAT, APT36, Mythic Leopard

Transparent Tribe, a suspected Pakistan-based threat actor, known for targeting government-based entities, majorly focusing on military personnel, and government servants, has now turned to target educational institutions and students based in India.

The malicious campaign started by the APT group in late December 2021, uses CrimsonRAT, one of its most common techniques, giving them long-term access to victim systems. These maldocs and malicious emails contain embedded links to infrastructure hosted on a Pakistan-based web service provider with names like student-portal to portray a real scenario. In addition to this infrastructure and malicious documents, there are several google drive and cloud-based drives with honeytraps setup to compromise students and probably compel them to involve themselves in leaking sensitive information for some institutes that have been engaging with the Indian government for defense research.

For further information, refer to Cisco Talos Intelligence's blog.

07

New Lightning Framework Targets Linux Machines

Tags: Lightning Framework, Linux, Malware

Intezer in its blog, revealed a new undetected Linux malware dubbed as Lightning framework. The malware, having multiple capabilities, has a modular approach with plugins available for different abilities and is also capable of installing rootkits.

Lightning framework consists of different modules and plugins like sshijacker, sshd, nethogs, some of which are open-source tools. The modules included are downloader and core modules, downloader module contacts the C2 to fetch the core module and plugins while using typosquatting and masquerading to remain undetected. Core is the main module of this framework, receiving commands from the C2 and executing them including plugin modules.

For IOCs, refer to Appendix 1C

08

Roaming Mantis Targets France via Smishing Campaign

Tags: Smishing, France, Roaming Mantis

Uncovering a smishing (SMS phishing) campaign actively targeting victims in France, an analyst at Sekoia.io shared some detailed insight on the campaign. The campaign uses embedded URLs which either deploy MoqHao Android malware or redirect to an Apple credential harvesting page.

On detailed analysis, it is observed to be like Roaming Mantis, and has compromised approximately 70,000 devices till date. MoqHao, aka XLoader is an Android RAT (Remote Access Trojan) capable of installing backdoors and stealing information.

The existing campaign starts with an incoming SMS on a victim's mobile, then accessing an embedded URL. Once this is done, according to the request, location, and device type, i.e., iOS or Android device is identified. According to this, Android malware or iOS credential harvesting page is redirected, post which for android devices MoqHao is executed, connecting to C2 server and performing further activities.

09

APT 29 Uses Cloud Storage Services for Malware Campaign

Tags: APT 29, Nobelium, Cloud services

APT 29, aka Nobelium or Cozy Bear, has been observed using online storage services, like Dropbox, and Google Drive to operate on a daily basis in order to avoid detections. The most recent campaigns by the group involve pdf campaigns targeting NATO countries in Europe. The document propagated as agenda.pdf is a supposed call out from the Ambassador of Portugal to the Ministry of Foreign Affairs of NATO countries.

The pdf contains different links which send out a beacon to a Dropbox account returning a malicious ISO file. Once this file is received, a shortcut file named agenda.lnk is executed, beginning a process and loading malicious DLL files. Once this stage is completed, the user information from the infected system is sent back to a Google drive share, followed by a returned cobalt strike payload to this system, and a connection is established via this payload to a C2 server.

For further information, refer to Palo Alto's blog.
For IOCs, refer to Appendix 1E.

10

Major Ransomware Attacks of the Month

01 Everest Ransomware targets Federal Bank/Fedfina (India) collecting 1130 GB of data.

02 BianLian Ransomware targets Veritas Solicitors, a company involved in legal issues in the UK.

03 Hive Ransomware targets Empress EMS, a company based out of New York.

Appendix

Appendix 1A – Hive Ransomware Variant

SHA256
f4a39820dbff47fa1b68f83f575bc98ed33858b02341c5c0464a49be4e6c76d3
88b1d8a85bf9101bc336b01b9af4345ed91d3ec761554d167fe59f73af73f037
065208b037a2691eb75a14f97bdbd9914122655d42f6249d2cca419a1e4ba6f1
33744c420884adf582c46a4b74cbd9c145f2e15a036bb1e557e89d6fd428e72
afab34235b7f170150f180c7afb9e3b4e504a84559bbd03ab71e64e3b6541149
36759cab7043cd7561ac6c3968832b30c9a442eff4d536e901d4ff70aef4d32d
481dc99903aa270d286f559b17194b1a25deca8a64a5ec4f13a066637900221e
6e5d49f604730ef4c05cfe3f64a7790242e71b4ecf1dc5109d32e811acf0b053
32ff0e5d87ec16544b6ff936d6fd58023925c3bdabaf962c492f6b078cb01914

Appendix 1B –Maui ransomware

Md5	4118d9adce7350c3eedeb056a3335346
	9b0e7c460a80f740d455a7521f0eada1
	fda3a19afa85912f6dc8452675245d6b
	2d02f5499d35a8dffb4c8bc0b7fec5c2
	c50b839f2fc3ce5a385b9ae1c05def3a
	a452a5f693036320b580d28ee55ae2a3
	a6e1efd70a077be032f052bb75544358
	802e7d6e80d7a60e17f9ffbd62fcbbeb
SHA256	5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e
	45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78
	56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19
	830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570
	458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456
	99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f
	3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878
	87bdb1de1dd6b0b75879d8b8aef80b562ec4fad365d7abbc629bcfc1d386afa6

Appendix 1C- Lightning Framework

File	SHA256
Lightning.Downloader	48f9471c20316b295704e6f8feb2196dd619799ed ec5835734fc24051f45c5b7
Lightning.Core	fd285c2fb4d42dde23590118dba016bf5b846625 da3abdbe48773530a07bcd1e
Linux.Plugin.Lightning.Sshd	ad16989a3ebf0b416681f8db31af098e02eabd25 452f8d781383547ead395237

Appendix 1D – MoqHao malware

IP Addresses
134.119.193[.]106
134.119.193[.]108
134.119.193[.]109
134.119.193[.]110
134.119.205[.]18
134.119.205[.]21
134.119.205[.]22
142.0.136[.]49
142.0.136[.]50
142.0.136[.]52
142.4.97[.]105
142.4.97[.]106
142.4.97[.]107
142.4.97[.]108
142.4.97[.]109
146.0.74[.]157
146.0.74[.]197
146.0.74[.]199
146.0.74[.]202
146.0.74[.]203
146.0.74[.]205

IP Addresses
146.0.74[.]206
146.0.74[.]228
192.51.188[.]107
192.51.188[.]108
192.51.188[.]109
192.51.188[.]142
192.51.188[.]145
192.51.188[.]146
27.124.36[.]32
27.124.36[.]34
27.124.36[.]52
27.124.39[.]241
27.124.39[.]242
27.124.39[.]243
91.204.227[.]19
91.204.227[.]20
91.204.227[.]21
91.204.227[.]22
91.204.227[.]23
91.204.227[.]24
91.204.227[.]25

IP Addresses
91.204.227[.]26
91.204.227[.]27
91.204.227[.]28
172.81.131[.]12
172.81.131[.]14
172.81.131[.]10
172.81.131[.]11
172.81.131[.]13
103.80.134[.]41
103.80.134[.]40
103.80.134[.]42
61.97.248[.]6
61.97.248[.]7
61.97.248[.]8
61.97.248[.]9
103.249.28[.]206
103.249.28[.]207
103.249.28[.]208
103.249.28[.]209
92.204.255[.]172
103.80.134[.]26

IP Addresses
103.80.134[.]27
103.80.134[.]29
103.80.134[.]30
103.80.134[.]31
103.80.134[.]33
103.80.134[.]34
103.80.134[.]37
103.80.134[.]38
103.80.134[.]51
103.80.134[.]52
103.80.134[.]53
103.80.134[.]54
103.80.134[.]55
103.80.134[.]58
115.91.26[.]2
192.51.188[.]101
192.51.188[.]103
192.51.188[.]106
192.51.188[.]111
192.51.188[.]14
91.204.227[.]79

IP Addresses
91.204.227[.]80
91.204.227[.]81
91.204.227[.]82
91.204.227[.]83
91.204.227[.]84
92.204.248[.]66

URLs
hxxps://imgur[.]com/user/shaoye99/about
hxxps://imgur[.]com/user/shaoye88/about
hxxps://imgur[.]com/user/shaoye77/about
hxxps://imgur[.]com/user/shaoye66/about
hxxps://imgur[.]com/user/shaoye55/about
hxxps://imgur[.]com/user/shaoye44/about
hxxps://imgur[.]com/user/shaoye33/about
hxxps://imgur[.]com/user/shaoye22/about
hxxps://imgur[.]com/user/shaoye11/about
hxxps://imgur[.]com/user/shaoye777/about
hxxps://imgur[.]com/user/shaoye666/about
hxxps://imgur[.]com/user/shaoye444/about
hxxps://imgur[.]com/user/shaoye333/about
hxxps://imgur[.]com/user/shaoye222/about
hxxps://imgur[.]com/user/shaoye111/about

Hashes
2e7acc13e9a9911cb5dd4057c5f0c343
293165e4734e4a7dfcac8887034526a0733eeefd
83ba2b1c0352ea9988edeb608abf2c037b1f30482bbc05c3ae79265bab7a44c9

Appendix 1E- APT 29 campaigns

Lure File Samples-PDFs
CE9802B22A37AE26C02B1F2C3225955A7667495FCE5B106113434AB5A87AE28A
F9B10323B120D8B12E72F74261E9E51A4780AC65F09967D7F4A4F4A8EABC6F4C
A0BDD8A82103F045935C83CB2186524FF3FC2D1324907D9BD644EA5CEFACBAAF

ISO File Samples
347715F967DA5DEBFB01D3BA2EDE6922801C24988C8E6EA2541E370DED313C8B
DE06CF27884440F51614A41623A4B84E0CB3082D6564EE352F6A4D8CF9D92EC5

EnvyScout Samples-HTML Files
0ED71B0F4F83590CCA66C0C9E9524A0C01D7A44CF06467C3AE588C1FE5B13118
CBE92ABB2E275770FDFF2E9187DEE07CCE1961B13C0EDA94237ACEEB06EEFBBD

Malicious DLLs
A018F4D5245FD775A17DC8437AD55C2F74FB6152DD4FDF16709A60DF2A063FFF
9230457E7B1AB614F0306E4AAAF08F1F79C11F897F635230AA4149CCFD090A3D
FBA3A311A4C0A283753B5A0CDCADD3FE19F5A1174F03CB966F14D04BBF3D73EE

Compressed Payload Files-Underscore Files
A018F4D5245FD775A17DC8437AD55C2F74FB6152DD4FDF16709A60DF2A063FFF
56CFFE5E224ACBE5A7E19446238E5BB9110D9200B6B1EA8B552984D802B71547

Appendix 1E- APT 29 campaigns

Decompressed in-memory payload
295452A87C0FBB48EB87BE9DE061AB4E938194A3FE909D4BCB9BD6FF40B8B2F0
BC9AD574C42BC7B123BAAAFB3325CE2185E92E46979B2FAADDD4BC80DDFAC88A

Infrastructure linked to samples
porodicno[.]ba/wp-content/Agenda.html
wethe6and9[.]ca/wp-content/Agenda.html
dropbox[.]com/s/raw/dhueerinrg9k97k/agenda.html

Cobalt Strike C2s
crossfity[.]com
techspaceinfo[.]com

Registry Keys
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AgendaE
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AdobeUpdate

Email Senders
matysovi@seznam[.]cz

Appendix 1E- APT 29 campaigns

Emails
761ED73512CB4392B98C84A34D3439240A73E389F09C2B4A8F0CCE6A212F529C
4C1ED0F6470D0BBE1CA4447981430E8CEB1157D818656BE9C8A992C56C10B541

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