Payatu

January 2023

Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

Table of Contents

01

WordPress Websites Targeted by Linux Backdoors

Tags: IT, WordPress, Linux

A Linux malware hacking the WordPress CMS-based websites was discovered recently by Doctor web, capable of exploiting 30 different vulnerabilities in various plugins and themes of the platform. WordPress, being one of the most used platforms, often attracts the attention of hackers and threat actors.

In the current scenario, malware targets outdated versions of plugins that can be injected with malicious JavaScript. Once a user clicks on such pages, they are redirected to other sites.

Vulnerabilities such as CVE-2016-10972, CVE-2019-17232, CVE-2019-17233 are few of the vulnerabilities used for compromising systems. Major plugins that are affected by these vulnerabilities are WordPress Ultimate FAQ, WooCommerce, and Google Code Inserter.

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

02

BitRAT Uses Compromised Sensitive Data to Lure Victims

Tags: Banking, Finance, Fintech, Malware, BitRAT

BitRAT, a notorious trojan sold over underground marketplaces and forums for a mere $20 for lifetime access, is being circulated around as part of multiple malicious campaigns to target banking infrastructure, especially in South America. Qualys in its report updated the community about how in different campaigns the threat actors are using sensitive data stolen from banks, that is available on the same marketplaces to lure victims.

In one instance shared by researchers, data of Columbian banks' infrastructure, was compromised using an excel file already containing sensitive data that was partially legitimate, making it difficult to detect. The excel sheet containing seemingly legitimate data contained obfuscated macro, used for initial payload delivery and execution. Through payload written to the temp folder, specific libraries like WinHTTP are called to download the payload which is stored as a repository on GitHub.

The downloaded payloads are .exe files which then execute and connect back to CnC servers, providing remote access to the victim machines for performing attacks.

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

03

Africa's French Speaking Banks Targeted by Threat Group BlueBottle

Tags: Banking, Finance, Fintech, GuLoader, Mimikatz, Bluebottle group

Using malware like GuLoader for initial attacks, Cobalt Strike, Keyloggers, and Ngrok for hosting C2 servers, the threat group named BlueBottle has been constantly targeting French speaking banks in Africa. Observed by researchers at Symantec-Broadcomm, the threat group was also monitored by Gorup-IB in 2019-2021 under the name OPERA1ER, where it compromised 30 targets and collected over $11 million.

The threat group uses the most common yet proficient tools available, along with techniques such as LOL (Living Off the Land). The victims are lured using French job-themed executables files, which are posed as pdf files, these deliver GuLoader, an anti-analysis capable shellcode downloader. The group has also been identified for using ISO files shared through CD-ROMs, another initial vector used is job-themed malware, delivering GuLoader, an anti-analysis capable shellcode downloader. As the success rate of the campaign by Bluebottle is high, it is likely to continue and accelerate the intensity of the attacks on African nations, as well as possibly other French speaking nations in the vicinity.

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

04

SpyNote RAT Targets Financial Institutions

Tags: Banking, Finance, Fintech, Malware, SpyNote

Belonging to the malware family SpyMax, the malware SpyNote and its variants have been targeting Android devices through various methods like Phishing, Smshing, and propagating fake applications of major Android applications. These applications include fake applications for different banks, like Kotak Bank, HSBC, Deutsche Bank, and everyday applications like WhatsApp, Facebook, and even Google Play.

Actively targeting the banking industry in the last quarter of 2022, the malware has introduced a new variant – SpyNote.C aka CypherRAT. Capable of both spying and collective bank data, the malware is discussed in detail by researchers at threatfabric. The variant can be used to exfiltrate PII data from banking customers, it can also be used to track SMS messages, call logs, video and audio recordings, and is also capable of installing new applications. This means that 2FA is compromised as the SMS can be shared to the C2 servers, while audio and video recordings compromise the privacy factor.

Tracking GPS location, extract codes from Authenticators such as Google Authenticator, and ability to use the Camera API in real time makes it a greater threat. China, India and the USA being the countries with most active Android users, makes it a major threat in these countries.

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

05

After Telecom, Now Australian Healthcare Industry Under Target

Tags: Healthcare, Malware, Gootkit Loader

Recently, the Gootkit loader, also known as Gootloader, has been observed in a series of attacks targeting organizations in the healthcare industry in Australia. This threat was originally known for utilizing search engine optimization (SEO) poisoning for initial access.

In response to findings of researchers at trendmicro, the Australian Cyber Security Center (ACSC) shared that they would conduct a review and communicate with any affected organizations. Previous reports by the team from July 2022 detailed the updated tactics used by Gootkit loader, such as its fileless delivery of harmful payloads and Cobalt deployment. The group's latest campaign suggests that it has additional malicious tricks.

To advance the infection process, the Gootkit loader leveraged VLC Media Player, a legitimate product also utilized by APT10. By downloading and executing malicious files from the internet, the malware maintains persistence using scheduled tasks in Windows, and sideloading malicious DLLs to inject processes. These connect back to C2 servers and execute legitimate tools.

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

06

DARK PINK, A New APT Group Targeting the APAC Region

Tags: APT Group, Sectors: Government, Non-Profit

In the 2nd half of 2022, GroupIB identified a new threat group targeting the APAC region, especially countries like Vietnam, Malaysia, Indonesia, Cambodia, Philippines, along with a few European countries. The major sectors targeted include Government agencies, religious organizations, etc. Involved in activities like cyber espionage, leaking sensitive information, recordings, and exfiltrating data, the group launches attacks through targeted spear-phishing emails posing as job applicants.

The group has developed some custom tools, namely, TelePowerBot, KamikakaBot, Cucky, and Ctealer stealers. Powersploit is the only publicly available tool involved in the group's operations. It is also subjected to use of less frequent techniques of the MITRE ATT&CK framework that is, Event Triggered Execution, along with other frequently used techniques such as DLL-SideLoading. The group has been observed to be using ISO images, Github Macros, and XML files in their operations during the initial stages, while exfiltration involves the use of Telegram mainly for sending ppt, pdf, and doc files. The second technique involved is extracting files via Dropbox, while specific files are shared via email to outlook based email-addresses.

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

7

Appendix

Appendix 1A – Linux Malware WordPress

MD5
c1620c4a48a3dcb1d27e587f456b371fc43bcb3d
9e6178d90f58e9459377a17a7ec2f5bedecd7515
6bcbd2a5dbfc9a5763c47b7eb327e7df35b401d1
c0053393f9dbe6113bef85dd88b02fa101df030c
c9f7cbc5e634370c396b88c74f426e7a82e23455
2e995ec1ecfd9b747174e9a19f43d3307c345382
4ecd9ce89864da0bb758b8a9564976bbe6235aa0
297e08c30bb487b2820c891e4c9628a04a4fafdc
3efbd95631e49828a43e8dc5b0035003c96c29b0
16c737e9d223b9349538e5366963744b3c811a25
f7ae703e2413600ecf2d0c3c20023a45958ab20b
3284c52eeb26abe796070645a1dabb4009fa61f7
616b98f0c7d28140c841ffb0acef4d0e7fd63abf
1e950dfa3f6e44a066b4228658e1de1152ba738e
215a4470063080696630fb6015378938e8c16a15
39dea5cb680488e2942641d85c53a80d3b6e03b7
077d581dbe356bd1ccb94d1833fa368e3f61b5ed
dfb751fa4c393e0748fe29450b0c9953d6c2e005
c4fcfe1599b2e145d7a4249bd9360968d0706ee2
565a1e98ef9ac549a8594b2e3777d378ef66251c
df4b067cbe01b1ff02aa9ccd5ae37b04830f3cd7
155171bfca23d3c25fe8b1ac211141c0d1216d62
e11628ab66e4616d22eb150d121ccf9710069474
d5f59dba969401c546ffc9b293223b9c6ce229df
c017a4b93e702120ec64befacfa085bd2d0f3a93
f402fb0b305ea3b65cbd6d6eeeb0084a434ce258

57a23460fb58c2198ec4acc6a6de79284650aa2d
d3c262d5a12e91921d5a09b746d51fc53e7fbc9f
076b8e6ef4f800aa458b627dc3caae63718ef6fb
4a54b885617dc613d28f071af58196f5197f0b5b
8bd3f72333f50962efaa01d927c6cbc3517d986e
eeb05978ede31b163912300ee05d45be9f2a0ccd
bc85aa5917c050311e8889dad3de9a77abdacf13
22a0c4debdb1f9f99d00b0f818da88f7429798a3
b581d939def9328b0d985b2b1df38cd25fc475d9
6cedba22594c52d5dd9c5b66ffa175c26ff06025
09a0d142eb51d2a59ebb88627b3579cfb2083f7b
c19bd1a1b2b18b48273cda326154a369fd07b96d
344ec12182ab2bf79a10dec7f7c27b3b0e0b2fa0
a3f6f731a0ca6455e4817aa7c68d47a0464691eb
e5bb95687d464ada71c9f06497140a57a8c03ec2
3e1204224b1492b06107a61ab7f11ad8b50ef456
fdeeb68a92a7805ecb7bb7f728d9f28f322a536f
acd4339fa505d9ff76d85633fcae4265ebebd135
215a4470063080696630fb6015378938e8c16a15

Domains
lobbydesires[.]com
letsmakeparty3[.]ga
deliverygoodstrategies[.]com
gabriellalovecats[.]com
css[.]digestcolect[.]com
clon[.]collectfasttracks[.]com
count[.]trackstatisticsss[.]com

IP
109[.]234.38[.]69
198[.]24.166[.]222
193[.]37.213[.]197
45[.]9.148[.]48

Appendix 1B – BitRAT

MD5
fd3822ff0c074b2d8f02973669525f3d
689b09ec2bc8c7cb409b82787af1a513
ff96bd13f7d654b6a5f358b904f34e94

Appendix 1C – Bluebottle group

SHA256	File
117c66c0aa3f7a5208b3872806d481fd8d682950573c2a7a-caf7c7c7945fe10d	ZIP file
c56c915cd0bc528bdb21d6037917d2e4cde18b2e-f27a4b74a0420a5f205869e6	Infostealer
91b3546dde60776ae3ed84fdf4f6b5fba7d-39620f0a6307280265cde3a33206b	.NET downloader
9c4c9fa4d8935df811cae0ce067de54ffdb5cfb4f99b4bc-36c5aa2a1ac6f9c8f	.NET downloader
1f6be4c29dfb50f924377444e5ca579d3020985a357533f-c052226f0091febf6	.NET downloader
d5b8009dcb50aac8a889e24f038a52fe09721d142a-3f1eaa74ac37fff45e9ba2	.NET downloader
ae4ff662c959cf24df621a2c0b934ed1fa1c26a270a180f-695cd5295579afbbd	.NET downloader
0612ef9d2239edeab05f421e3188e2cfcadacbaeafbc-9b8e35e778f7234aaa3b	.NET downloader
4acd4335ca43783ff52c0ccbb7e757ea14fb261c-33d08268e85ed0ac34e0abec	.NET downloader

47718762dc043f84fb641b1e0a8c65401160cc2e558fd-38c14d5d35a114b93cb	.NET downloader
a539961f80feb689546a2e334b03aed81252 04fae032e2d28ed9a7000b3afff	.NET downloader
07ca6122fde46d48f71bcde356d5eeb89040e-4a6e83441968a9dade98dc36fe5	.NET loader
938f50cb2e2d670497209e8cef5bf1042f752b6bf76d1547d-68040b5a27f618b	.NET loader
a257eeebba15afecf76b89a379e066e5ed79a2bb-9da349c1fdb5a24316abc753	GuLoader
f276c6a25d6b865c6202978f1d409e8b74e063263eab517f-249cf6d3ad3fae4a	GuLoader
3d0fd0444a9e295135ecfdc8c87ddc6dcdff63969c745e-0218469332aef18dfe	GuLoader
ac98e6bf6d16904355b1c706bc2b79761a8b09044da40f2c-8bce35142ef8bcc8	GuLoader
ca75b0864d8308efe94eb0822de55eb7f-5cfd482d2190100dfd00d433ee790a0	GuLoader
088110b0ee3588a4822049cf60fff31c67323a9b5993eae-3104cc9737a47ce0c	GuLoader
b4adbb5d017d6452c2e1700584261cd3170ee-5a14ac658424945f15177494ba1	GuLoader
818284e7ea0a4bd64ba0eda664f51877ed-8c6d35bf052898559dbf4ad8030968	GuLoader
fa6ca0a168f3400a00dc43f1be07296f4111d7ad-9b275809217a9269dd613ae8	GuLoader
d5b3b1304739986298ba9b7c3ff8b40b3740233d6bb-02437ce61a20ee87468bc	GuLoader
8495a328fdd4afd33c3336e964802018d44c1dda15b-804560743d6276e926218	GuLoader
ce2ea1807d984e1392599d05f7ab742bae4f20f8ef-80c5a514fbdeede2ff7e55	Quasar RAT
e933ec0f52cbc60b92134d48b08661b1af25c7d93ff5041f-c704559b45bd85b8	Netwire RAT
6db5e2bb146b11182f29d03b036af4e195044f0ef7a8f-7c4429f5d4201756b8f	Cobalt Strike
f4fba2181668f766fdfbd1362420a53ac0b987f999c95baf5d-be235fd3bad4b8	Cobalt Strike
ec2146655e2c04bf87b8db754dd2e92b8c48c4df-47b64a9adc1252efd8618e62	Fakelogon-screen

5090f311b37309767fb41fa9839d2770ab382326f38bab8c-976b83ec727e6796	SharpHound
5e245281f4924c139dd90c581fc79105ea19980baa68eec-cf5bf36ae613399b9	PsExec
31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01ae-c4d5ba01d539a0fc	Mimikatz

Network Indicators
hxxp://files[.]ddrive[.]online:444/load
hxxp://85.239.34[.]152/download/XWO_UnBkJ213.bin
hxxps://transmissive-basin[.]000webhostapp[.]com
hxxps://udapte[.]adesy[.]in
banqueislamik[.]ddrive[.]online
hxxps://transfer[.]sh/get/mKwvWI/NHmZJu.rtf
hxxps://transfer[.]sh/get/RTPlqa/oISxUP.rtf
hxxp://files[.]ddrive[.]online:4448/a
hxxp://banqueislamik[.]ddrive[.]online:4448/ZPjH
hxxp://46.246.86[.]12/ca3.exe
hxxp://178.73.192[.]15/ca1.exe
personnel[.]bdm-sa[.]fr
185.225.73[.]165

Appendix 1-D SpyNote

App name	Package name	SHA-256
HSBC UK Mobile Banking	com.employ.mb	6f606bc5004af2b90b-66d6e6e4f29f35a3b4a31d-c6974b55434b3c-53d70584a4
Deutsche Bank Mobile	com.reporting.efficiency	114fa822d7a96169c-9cd48303f7fbd1af94f57cb-46fec576d91ccea11bc5d974

BurlaNubank	com.appser.verapp	34d70ce1e9eeafd-c225abbfa84c24454986a-47ca7a41431c-38ca16e612d3f818
Kotak Bank	splash.app.main	bd172dbb47a95e7abc-3ce76118bf6cd3f742d-7c932ec8801cd553509f31e-ca8e
Bank of America Confirmation	yps.eton.application	2e1c68c3e785679c-04d915eb2f960ef5e7ef-3294a423e1835aa06e-0254812c7a
CypherRat	com.appser.verapp	4779c469c50d157d2140d39f-c9b034c931b5224e886bcb-60024687fe4022063e
Virtual SimCard	cobi0jbpm.apvy8vjjvpser.verap-chvvhbjbjq	a2a95cfccb8fbe557f-605b8a47dad901d3a25f8c-dae7f0beee133f60b924c45a
Current Activity	com.willme.topac-tivity	bade089b4df-dea057132551deb-997ba8a25c4d1ced32f-78975239c73241181f4
Conversations_	com.appser.verapp	bf4e003360cb2024d-faa46a79bf05f667d300f2b-cd0765b9a12500201b9519a7

Host	Port
bizebiz.myftp.org	6378
adnankara1.ddns.net	7771
silent911-44688.portmap.io	44688
154.211.96.78	8088
159.203.126.35	22526

Appendix 1-E Gootkit Loader

File name	SHA256	Detection
libvlc.dll	7c2ea97f8fff301a03f36fb6b87d08dc81e-948440c87c2805b9e4622eb4e1991	Trojan.Win64.COBE-ACON.SWG
Object Relations.js	6d549cd0b623f5623bb80cc344f6b73962d-76b70a7cbd40ca8f1d96df7cce047	Trojan.JS.DOWNLOADER.AC
PSHound.ps1	a9d2a52e418f5cc9f6943d-b00a350a5588c11943898d3d6d275e1b636b-3cd7c8	HackTool.PS1.BloodHound.C
so.ps1	57af5c9f715d-5c516e1137b6d336bff7656e1b85695fff-4c83fc5a78c11fdec6 575c516e1137b6d336bff7656e1b85695fff-4c83fc5a78c11fdec6	Trojan.PS1.POWLOAD.TIAOENO

Network Indicators
193[.]106[.]191[.]187
hxxp://bip.podkowalesna [.] pl/xmlrpc.php
hxxp://blog.ddlab [.] net/xmlrpc.php
hxxp://bodilbruun [.] dk/xmlrpc.php
hxxp://clearchoiceairtreatment [.] com/xmlrpc.php
hxxps://ahanpt [.] ir/xmlrpc.php
hxxps://allthetech [.] com/xmlrpc.php
hxxps://baban [.] ir/xmlrpc.php
hxxps://centre-samekh [.] ch/xmlrpc.php
hxxps://covid19.gov[.]gd/xmlrpc.php
hxxps://educabla [.] com/xmlrpc.php
hxxps://emitrablog [.] com/xmlrpc.php
hxxps://fx-arabia [.] com/xmlrpc.php
hxxps://mangayaro [.] com/xmlrpc.php
hxxps://mgplastcutlery [.] com/xmlrpc.php
hxxps://nmm [.] pl/xmlrpc.php
hxxps://ntumatches [.] tw/xmlrpc.php

hxxps://ruscred [.] site/xmlrpc.php
hxxps://sayhueque [.] com/xmlrpc.php
hxxps://thedinkpickleball [.] com/xmlrpc.php
hxxps://www.slimdiet [.] eu/content.php
hxxps://www.studio-lapinternet[.]fr/content.php
hxxps://yespornplease [.] tv/xmlrpc.php

Appendix 1F – DarkPink APT

Cucky
926027F0308481610C85F4E3E433573B
24F65E0EE158FC63D98352F9828D014AB239AE16
9976625B5A3035DC68E878AD5AC3682CCB74EF2007C-501C8023291548E11301A
Ctealer Loader
728AFA40B20DF6D2540648EF845EB754
D8DF672ECD9018F3F2D23E5C966535C30A54B71D
C60F778641942B7B0C00F3214211B137B683E8296ABB1905D2557BFB245BF775
Packed Ctealer
7EAF1B65004421AC07C6BB1A997487B2
18CA159183C98F52DF45D3E9DB0087E17596A866
E3181EE97D3FFD31C22C2C303C6E75D0196912083D0C21536E5833EE7D108736
732091AD428419247BCE87603EA79F00
142F909C26BD57969EF93D7942587CDF15910E34
E45DF7418CA47A9A4C4803697F4B28C618469C6E5A5678213AB81DF9FC-C9FD51

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