Payatu

October 2023

Cyber Threat Intelligence Report

Payatu Security Consulting Pvt. Ltd.

Table of Contents

A.
Ransomware Statistics 03

B.
GHOSTPULSE: Stealthy Campaign Targeting MSIX Packages 05

C.
Winter Vivern's Escalated Cyberespionage Against Government Email Servers 06

D.
Vietnamese Cybercrime Groups Target the Digital Marketing Sector 07

E.
Kaspersky's Global APT Threat Report 2023 08

F.
D-Link Claimed to have Breached, Company Shares an Update 09

G.
Malicious Campaigns Target Binance Smart Chain 10

H.
Void Rabisu's Expanding Cyber Threat 11

I.
The GoldDigger Android Trojan Targets Vietnam 12

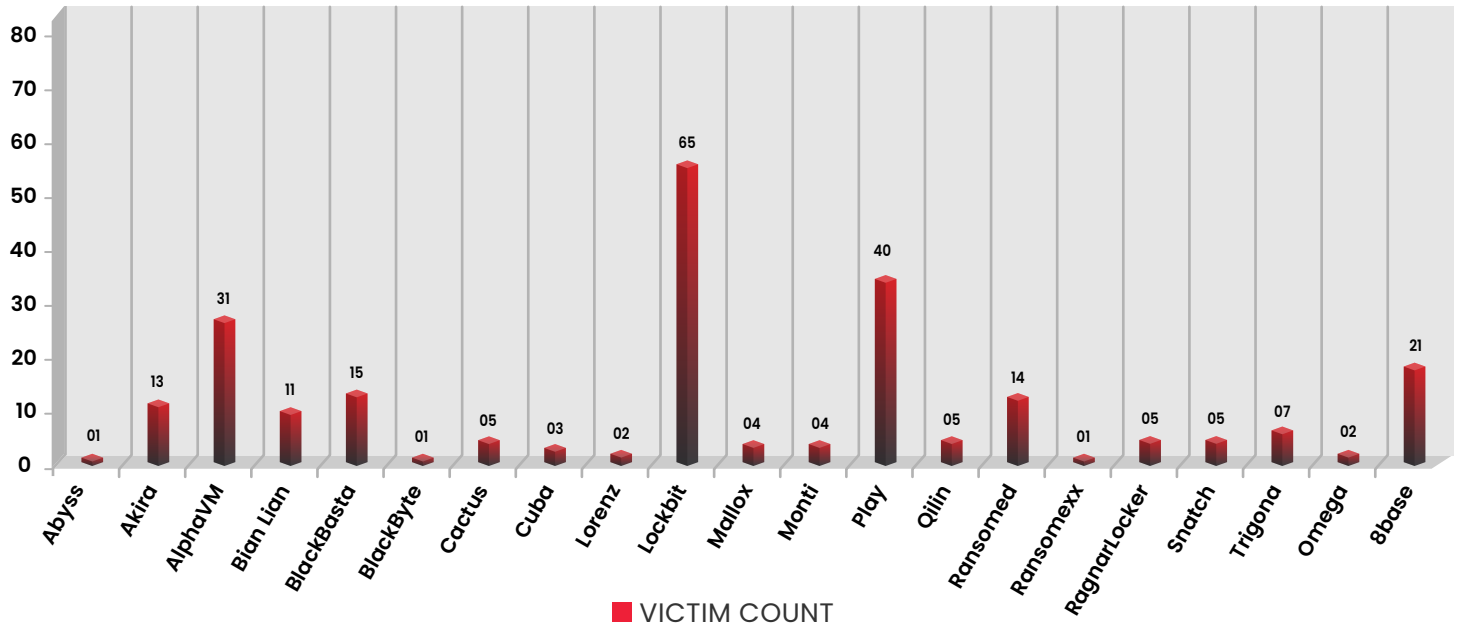
J.
Appendix 15

01

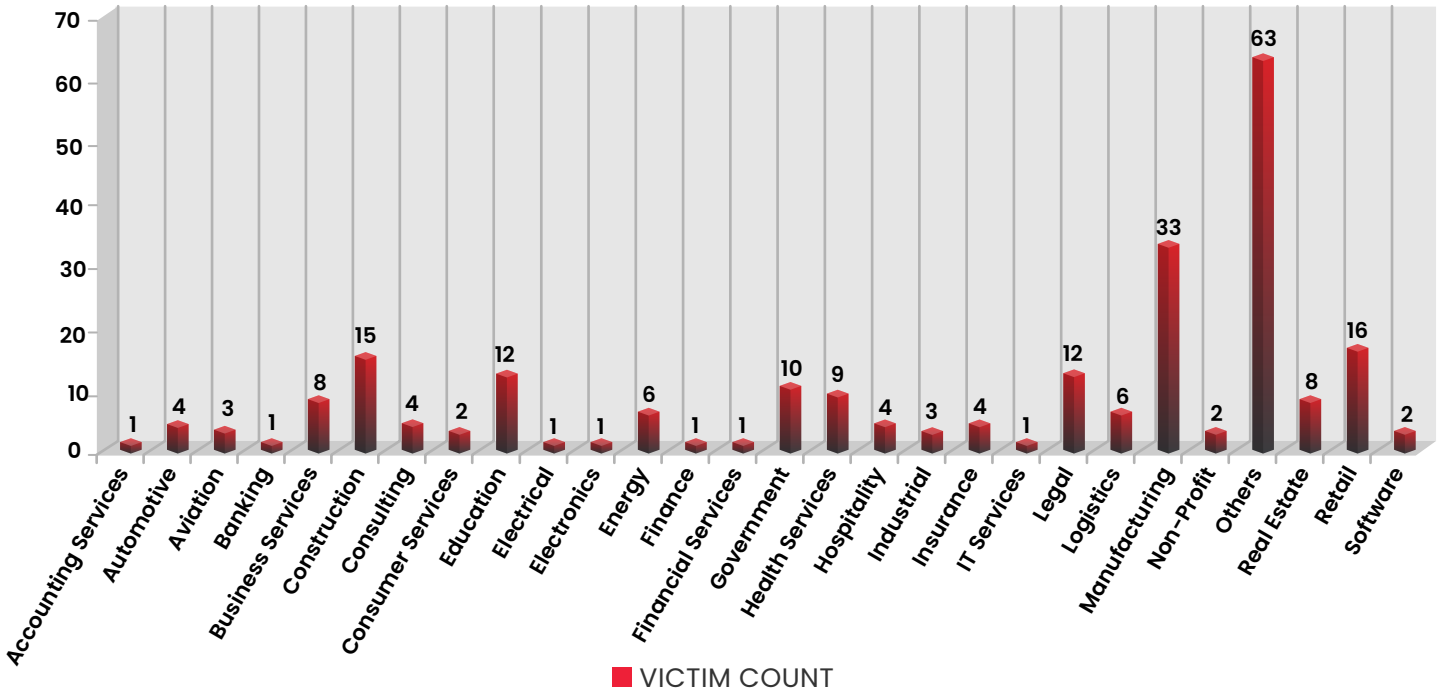
Ransomware Statistics

- Air Canada claimed to be hacked by Bian Lian
- German giant Haffner claimed to be compromised by Blackbasta
- United Kingdoms Royal College of Physians and Surgeons claimed to be compromised by Akira
- AVA Ltd. claimed to be compromised by 8base

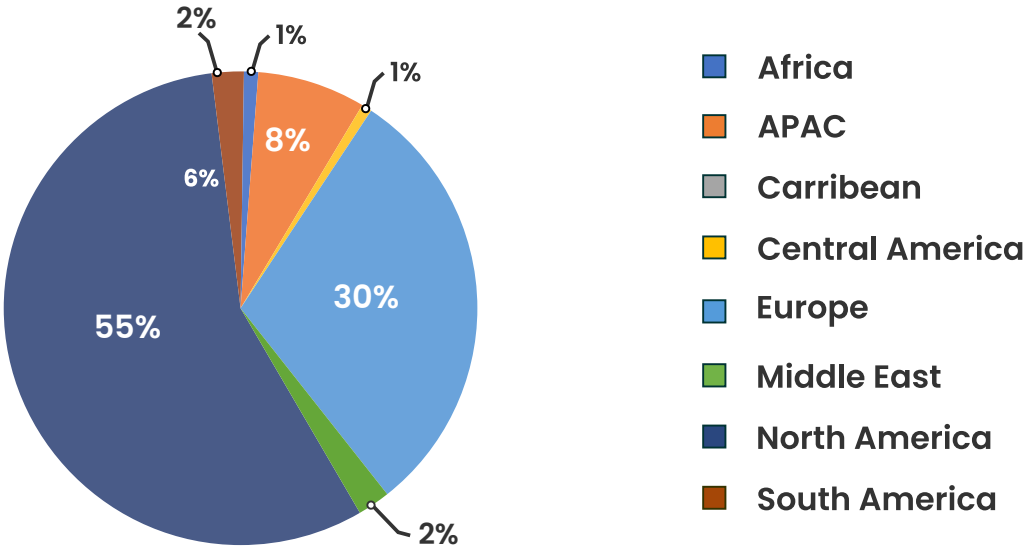
ATTACKS TREND BY RANSOMWARE



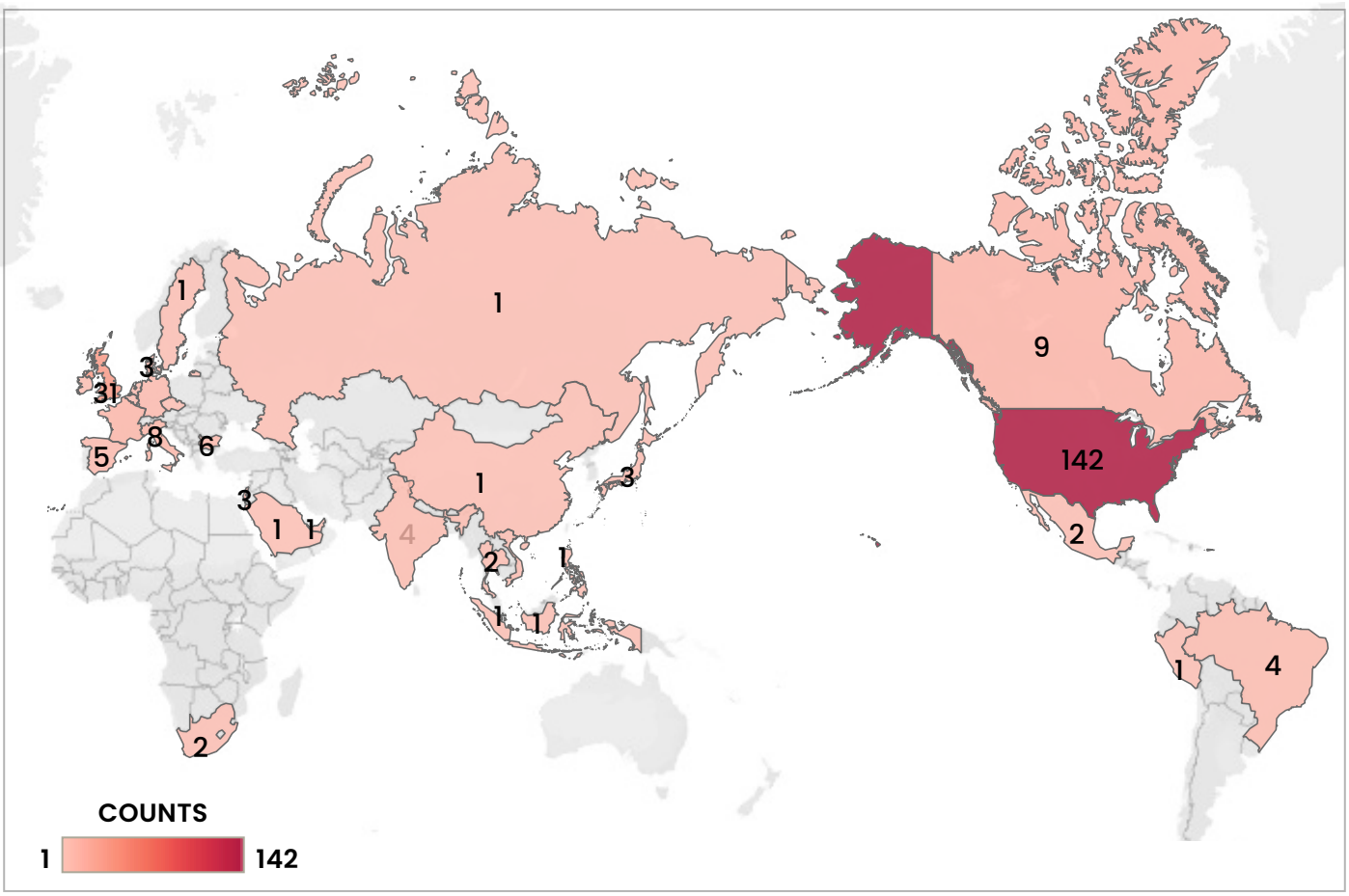
SECTOR-WISE ATTACK TREND



REGION-WISE ATTACK



COUNTRY-WISE ATTACK TREND - 255



02

GHOSTPULSE: Stealthy Campaign Targeting MSIX Packages

Tags: Malware

Elastic Security Labs has identified a malicious campaign using signed MSIX application packages to breach user systems. MSIX, a Windows application package format, allows developers to distribute and install their software with a simple double-click. Due to its ease of use, cyber adversaries are targeting it, especially those with access to stolen or purchased code signing certificates. Users are lured into downloading these malicious packages from compromised websites, search engine manipulations, or deceptive ads with counterfeit themes like Chrome, Brave, and Grammarly installers.

The campaign employs a loader named GHOSTPULSE, which functions in stages to deliver its final payload undetected. Initially, a PowerShell script, termed as 'stage 0 payload,' is sometimes used. GHOSTPULSE then moves through three stages:

- Embedding within a malicious DLL activated during DllEntryPoint.
- Creating a new IAT structure and utilizing the CRC32 hashing method.
- Loading and executing the final payload in a different process, while simultaneously altering its own instructions for obfuscation.

The endgame for GHOSTPULSE is to introduce an information-stealing payload, examples being SectopRAT and Lumma.

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

03

Winter Vivern's Escalated Cyberespionage Against Government Email Servers

Tags: Winter Vivern, Europe, Government

ESET Research has documented Winter Vivern's cyberespionage activities for over a year, and on October 11th, 2023, the group exploited a new zero-day XSS vulnerability in the Roundcube Webmail server, distinct from the previously exploited CVE-2020-35730. Winter Vivern has persistently targeted governmental email servers, specifically Zimbra and Roundcube, since 2022. Its activities in August and September 2023 centered on exploiting the CVE-2020-35730, an XSS vulnerability in Roundcube. Interestingly, another group, Sednit (APT28), also exploited this old vulnerability, occasionally targeting the same entities.

The new XSS vulnerability, dubbed CVE-2023-5631, allows remote exploitation through a specifically designed email. In Winter Vivern's campaign, such emails originated from team.managment[@]outlook[.]com with the subject "Get started in your Outlook".

Although Winter Vivern previously exploited known vulnerabilities with available proofs of concept, its adoption of a zero-day vulnerability marks an operational escalation. Despite its basic toolset, the group poses a considerable threat to European governments due to its tenacity, frequent phishing campaigns, and the prevalent neglect in updating vulnerable, internet-facing applications.

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

04

Vietnamese Cybercrime Groups Target the Digital Marketing Sector

Tags: Digital Marketing, UK, USA, India

Vietnamese cybercrime factions are intensively targeting the digital marketing sector, utilizing Malware as a Service (MaaS) infostealers and Remote Access Trojans (RATs) with an aim to hijack Facebook business accounts. The methods and targets of these groups significantly overlap, hinting at a coordinated cluster of operators.

WithSecure's Detection and Response Team discovered multiple DarkGate malware attacks on its customers across the UK, US, and India. These tactics were eerily like the DuckTail infostealer campaigns, pointing towards the same perpetrator.

The prevalent overlap of tools is attributed to the cybercrime marketplace where threat actors can easily buy and deploy various tools. Relying only on tools for identification might be misleading, as different actors can use the same tool. However, tracking them via unique non-technical markers, like specific lure topics, provides a more comprehensive view.

A peculiar file named "job description*.zip" emerged as a significant identifier, leading to the discovery of malicious files mimicking brands like Prada and exploiting the finance company, Groww.

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

05

Kaspersky's Global APT Threat Report 2023

Tags: Sandman, Lua, Middle East, Asia

Kaspersky's Global Research and Analysis Team (GReAT) has provided insights into Advanced Persistent Threat (APT) activities during Q3 2023:

Compromised USB Drives in APAC: In early 2023, an attack targeting APAC government entities was uncovered. It exploited a type of secure USB drive, utilizing sophisticated tools like virtualization-based software obfuscation, direct SCSI commands for USB communication, and injection of code into the USB drive's access management program. BlindEagle's Expanding Targets: primarily targeting South American government entities and individuals for espionage and financial data theft, BlindEagle has frequently changed its choice of open-source remote access Trojans (RATs) like AsyncRAT and Lime-RAT.

Emerging APT Group in Russia: An unidentified group began targeting Russian entities in late 2022 through spear-phishing emails, deploying a Trojan designed for data exfiltration and command execution. A malicious campaign based out of China named "GOFFEE" was identified, targeting Russian entities using the Owowa Trojan and an email-based intrusion chain reminiscent of CloudAtlas activity. TargetPlug is another malware originating from China, an in-memory implant, TargetPlug, primarily attacked South Korea's gaming sector. By April, related variants re-emerged.

Active since 2012, Dark Caracal's cyber-espionage campaigns originating from the Middle East, spans governments, militaries, and various industry sectors globally. Known since 2012, Strong Pity, another Middle Eastern target, previously attacked Italian and Belgian users with malicious software versions.

Lazarus's ongoing campaign involves trojanized apps, including backdoored VNC apps, to access systems. It deceives job seekers into opening these apps, leading to malware deployment.

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

06

D-Link Claimed to have Breached, Company Shares an Update

Tags: D-Link

On October 2nd, 2023, D-Link Corporation was alerted about a potential data breach claim made on an online forum. Swiftly responding to the allegation, the company initiated an in-depth investigation and engaged external experts from Trend Mirco to assess the situation. These investigations revealed several inaccuracies in the online claim.

The supposed breach was not from the cloud but traced back to the D-View 6 system, which became obsolete in 2015. The data primarily consisted of registration details, devoid of user IDs or financial data. It contained around 700 records, contrary to the claim of "millions of users' data." Most data included low-sensitivity and semi-public information, like contact names or office emails.

The incident was likely due to an employee inadvertently falling for a phishing scam, granting unauthorized access to outdated records. Though D-Link's systems were compliant with then-prevailing security standards, the company deeply regrets the oversight and has since bolstered its security measures, including terminating the services of the implicated test lab.

Despite the incident, D-Link assures that current customers are unlikely to be impacted. The company remains committed to data security and urges customers to contact local customer service if they have concerns. D-Link reminds its users that it never asks for passwords or financial information via calls, texts, or emails and advises them to report any such suspicious communication to local authorities immediately.

07

Malicious Campaigns Target Binance Smart Chain

Tags: Binance

Guardio Labs detected the "ClearFake" malware campaign, which deceives users through defaced websites prompting a deceptive browser update, subsequently introducing malicious infostealer malware. Attackers compromise WordPress sites by implanting a concealed JavaScript code, which then fetches a secondary payload from an attacker-controlled server, further modifying the site. This process allows attackers to remotely adapt their tactics, including changing blocked domains without revisiting compromised WordPress sites.

While CloudFlare temporarily halted the campaign by blocking accounts, recent developments in the campaign showed traffic directed to Binance-controlled servers. Attackers exploit vulnerabilities in WordPress by targeting outdated plugins or versions. Using the Binance Smart Chain, attackers leverage the eth_call method for a stealthy, traceless method of fetching the malicious script. Protecting against such attacks necessitates regular WordPress and plugin updates, strong password protocols, and vigilant site monitoring. The misuse of blockchain poses challenges, as its properties can facilitate various malicious activities, evading traditional countermeasures.

08

Void Rabisu's Expanding Cyber Threat

Tags: Europe, ROMCOM, Malware

Void Rabisu is recognized for ransomware attacks and targeted operations against Ukraine and its allies, including the Ukrainian government, military, utilities, and EU figures. In 2023, its focus expanded to EU military and leaders promoting gender equality. Its hallmark tool, the ROMCOM backdoor, evolved with enhanced evasion features.

Emulating an Advanced Persistent Threat (APT) profile, Void Rabisu tapped into a zero-day flaw, CVE-2023-36884, leveraging significant events like the Ukrainian World Congress for decoy. The geopolitical tension around Ukraine seems to have shifted its activities from just financial motives to espionage.

Both Microsoft and Trend Micro pinpointed Void Rabisu's exploitation of the CVE-2023-36884 vulnerability against European establishments in 2023. Its tactics included creating a deceptive website, wplsummit[.]com, which offered a malicious executable with photos sourced from social media. Moreover, its PEAPOD samples modified WinHTTP operations, possibly complicating Command & Control tracking, with its exact intent remaining a puzzle.

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

09

The GoldDigger Android Trojan Targets Vietnam

Tags: GoldDigger, APAC

In August, Group-IB's researchers identified a new Android Trojan, codenamed GoldDigger, targeting financial institutions in Vietnam. This Trojan, active since June 2023, masquerades as a fake Android application, imitating a Vietnamese government portal and a local energy company. Its primary aim is to steal banking credentials. GoldDigger exploits the Accessibility Service to access personal data, intercept SMS messages, and execute user activities, and it possesses remote access capabilities.

A distinctive feature of GoldDigger is its advanced protection mechanism through Virbox Protector, a genuine software. This protection allows the Trojan to hinder both static and dynamic malware analyses and dodge detection. Using VirBox as a shield by banking Trojans is emerging, with three Android Trojans, including GoldDigger, recently adopting this method in the Asia-Pacific region.

GoldDigger is disseminated via counterfeit websites mimicking Google Play and Vietnamese corporate sites. Likely, smishing or traditional phishing strategies distributed these links. Though Android devices typically prevent app installations from third-party sources, if the "Install from Unknown Sources" setting is enabled, this Trojan can breach such barriers. GoldDigger, utilizing Accessibility Service, provides extensive invasive functionalities, including user interactions simulation, device screen unlocking, and even bypassing 2-factor authentication. GoldDigger is among several Android malware strains active in the Asia-Pacific, with others like Gigabud and SpyNote also posing threats.

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

11

Appendix

APPENDIX 1A – GHOSTPULSE RAT

Observable	Type	Name
78.24.180[.]93	ip-v4	
manojsinghnegi[.]com	domain-name	
manojsinghnegi[.]com/2.tar.gpg	url	
0c01324555494c35c6bbd-8babd09527bf-c49a2599946f3540bb3380d7be-c7a20	sha256	Chrome-x64.msix
ee4c788dd4a173241b60d4830db-128206dcfb68e79c68796627c6d-6355c1d1b8	sha256	Brave-x64.msix
4283563324c083f-243cf9335662ecc9f1ae102d-619302c79095240f969d9d356	sha256	Webex.msix
eb2addefd7538cbd6c8eb42b-70cafe82ff2a8210e885537cd-94d410937681c61	sha256	new1109.ps1
49e6a11453786ef9e396a-9b84aeb8632f395477abc-38f1862e44427982e8c7a9	sha256	38190626900.rar

APPENDIX 1A – GHOSTPULSE RAT

SHA-1	Pseudo name	Description
97ED594EF2B5755F0549C-6C5758377C0B87CFAE0	checkupdate.js	JS/WinterVivern.B
8BF7FCC70F-6CE032217D9210EF30314DDD6B8135	N/A	JS/Kryptik.BIK

IP Address	Domain	Hosting Provider	Description
38.180.76[.]31	recsecas[.]com	M247 Europe SRL	Winter Vivern C&C server

APPENDIX 1C – DARKGATE MALWARE

IP Addresses
117.0.194[.]195
149.248.0[.]82
158.160.81[.]26
162.243.71[.]6
167.114.199[.]65
178.33.94[.]35
179.60.149[.]3
185.141.60[.]18
185.143.223[.]64
46.173.215[.]132
5.188.87[.]58
5.34.178[.]21
66.42.63[.]27
80.66.88[.]145
82.117.252[.]140
89.248.193[.]66
94.228.169[.]123
94.228.169[.]143

Domains
Alianzasuma[.]com – Noisy but hosted malicious files
sanibroadbandcommunicton.duckdns[.]org

APPENDIX 1D – VOID RABISU

URL	Description
hXXps://onedrive[.]live[[.]]com/?auth-key=%21AAdO%2Di5%2DikrnuaA&id=79E2A760F4732317%21106&cid=79E2A760F4732317	OneDrive
wplsummit[.]com	Fake WPL Summit page
hxxps://mctelemetryzone[.]com/favicon[.]ico	Second stage downloader
netstaticsinformation[.]com	ROMCOM C&C
redditanalytics[.]pm	ROMCOM modules
wirelessvezion[.]com	Suspected ROMCOM C&C
budgetnews[.]org	ROMCOM C&C
pap-cut[.]com	Malware hosting
speedymarker[.]com	SEO domain
kayakahead[.]net	SEO domain

SHA-256	Filename Description
4f66d6ec70a49aaddb8018af1b-f859284a6a4a27eb2615c80a32d-5c7c156e476	Unpublished Pictures - !st Stage Downloader
4299c16e11a725dd2ac9468c5c0aab-f94ea5a90d2232810c19ba13b35b3708f9	favicon.ico - 2nd Stage Downloader
3c014d59cf22acbd062a4e2cab8cb8ede-7127b6a69af9db45a7dcefde866369a	favicon.ico - 2nd Stage Downloader decrypted
41e995a8554fb6e-4160d0e445856221ece2117a-2b030012ead9efe76611bdc14	Security.dll - 3rd Stage Malware
d1ca5349da287dbb13a1ea2a2982d23e-6ce34ed822baee7468ce1980a4179d42	OneDriveService.dll - 3rd stage malware
83448756a4cafbfd784d36add719cf-fa65b912e550d3a5fd63d407201c6ff94c	pcmf-installer-23.0.5.exe - ROMCOM 3rd Stage downloader

APPENDIX 1D – VOID RABISU

C&C
cskh[.]evnspa[.]cc
cskh[.]evnspc[.]cc
cskh[.]evnspe[.]cc
cskh[.]evnspo[.]cc
cskh[.]evnspr[.]cc
viet[.]cgovn[.]cc
viet[.]egovn[.]cc
viet[.]gdtgovn[.]com
viet[.]govn[.]cc

vietcp[.]cc
vietgav[.]cc
vietgov[.]cc
vietgov0[.]cc
vietgov1[.]cc
vietgov22[.]cc
vietgov3[.]cc
vietgov33[.]cc
vietgov4[.]cc
vietgov5[.]cc
vietgov6[.]cc
vietgovn[.]cc
viettgov[.]cc
vitgov[.]cc
hds6y[.]cc
ks8cb[.]cc
ms2ve[.]cc
smgeo[.]cc
wbke[.]cc
www[.]dg1e[.]com
zu7kt[.]cc

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.