Payatu

August 2022

Cyber Threat Intelligence Report

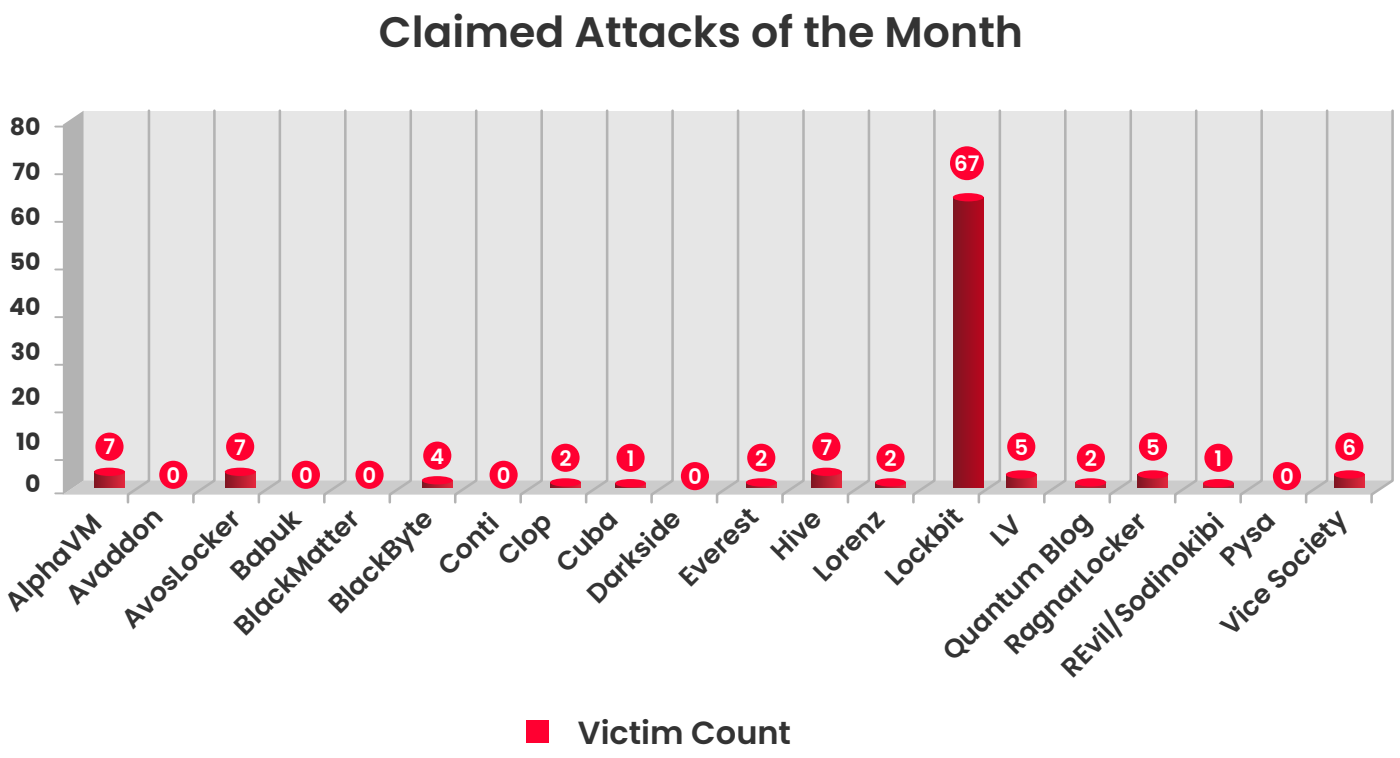
Payatu Security Consulting Pvt. Ltd.

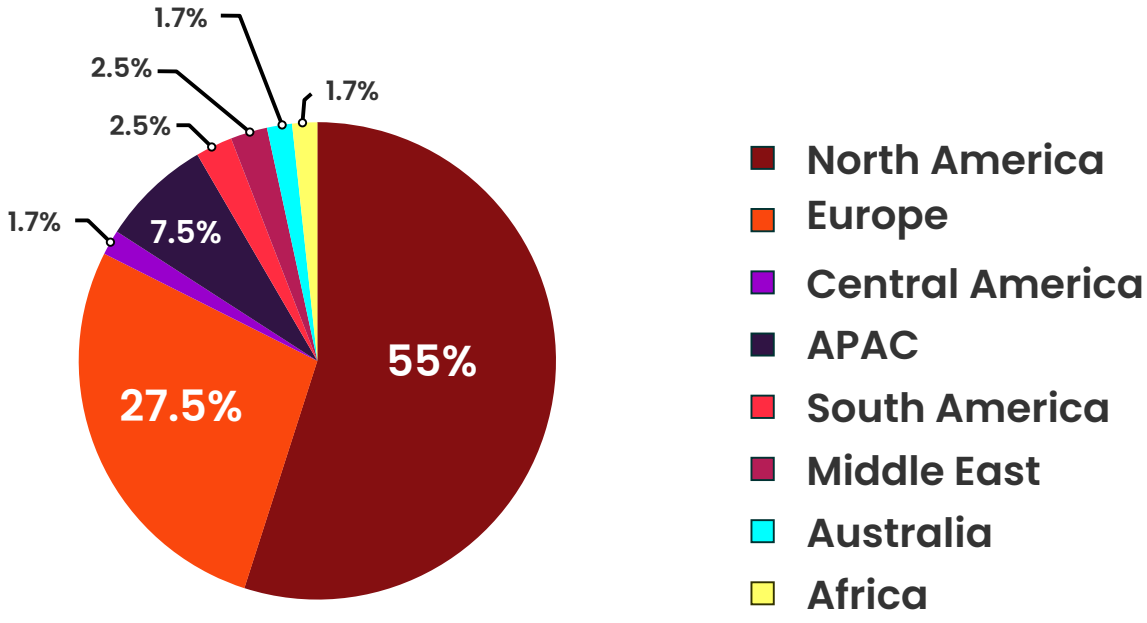
Table of Contents

01

Ransomware Statistics

- Yanluowang ransomware claims to have compromised Cisco stealing 2.8 GB of data.
- RagnarLocker ransomware claimed to have compromised DESFA pipeline - Greece.
- Vice Society claimed to have compromised FMC (Family Medical Centers) clinics.
- LockBit 3.0 ransomware claimed to have compromised Entrust Datacard Corporation.





Claimed Attacks of the Month

 USA - 59

 Italy - 6

 UK - 4

 Spain - 4

 Germany - 6

 Canada - 7

 France - 2

 Mexico - 1

 China - 3

 Montenegro - 1

 Singapore - 2

 Brazil - 2

 Luxembourg - 1

 Malaysia - 2

 Nicargua - 1

 Vietnam - 1

 Bulgaria - 1

 Qatar - 1

 Finland - 2

 Australia - 2

 Switzerland - 1

 Morrocco - 1

 Netherlands - 2

 Colombia - 1

 Portugal - 2

 Gabon - 1

 Israel - 1

 Greece - 1

 South Korea - 1

02

New Chinese Cobalt Strike-like Framework, Manjusaka

Tags: Cobal Strike, Manjusaka, Offensive Framework

Recently, researchers at Cisco Talos have identified a new attacking framework, named 'Manjusaka'. Given the tracking techniques used by defenders, it is highly important for threat actors to upgrade to new frameworks, and for pentesters to regularly follow any new frameworks. With implants written for Windows & Linux in Rust and C2 setup written in Golang with User Interface written in Simplified Chinese, the framework is possibly created for China-based threat actors, while also available for custom configurations.

'ManjuSaka', which means 'Cow Flower' in Simplified Chinese, is freely available on GitHub, was initially identified when researchers were analyzing a maldoc containing a Cobalt Strike beacon. The implants created are capable of RAT (Remote Access Trojan) like functionalities and a file management module. Following the infection via implant in a victim system, the RAT performs activities like arbitrary command execution, retrieve file information, network details, collect browser credentials, screenshot capable and establish connection with C2.

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

03

Microsoft Security Tools-based LOL Techniques Used by Lockbit Ransomware

Tags: Living off the Land, LOLBins, Lockbit, Microsoft

The new variant of Lockbit ransomware, Lockbit 3.0, reportedly launched in late June 2022, is being used widely as a RaaS, and is now using Windows Defender tools to load Cobalt Strike payloads. This is being done using Windows Defender command line tool –MpCmdRun[.]exe and VMWare command line utility VMwareXferlogs.exe.

After the initial compromise, various post-exploitation tools are run, like Meterpreter, PowerShell Empire and via these tools through Cobalt Strike. Once obtaining sufficient privileges, the ransomware side-loads malicious DLLs to these tools, which are then used to decrypt the beacons. Due to this ability, it makes detection of such malicious activities tough, and ransomware can easily evade security tools.

For further details, refer to Sentinel One's blog.

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

04

Follina-based LOL Techniques Used in the Wild

Tags: Follina, LOL Techniques, CVE-2022-30190

Another Windows-based attack vector being used is exploitation of Follina exploit, this RCE (Remote Code Execution) attack is a flaw identified in MSDT (Microsoft Support Diagnostic Tool). Even though a patch for the same has been shared by Microsoft, unpatched systems still are a risk to organizations.

In their research, Reversing Labs share that they have identified three different attack chains using Follina exploit for gaining a foothold, along with common exploitation techniques such as Mimikatz, Cobalt Strike and custom-made PowerShell scripts. The first chain uses a Microsoft Word document to call a third-party website invoking a HTML payload. This payload contains an embedded JavaScript with Base-64 encoded data, which calls msdt.exe and then logs into a remote server to execute a osupdate.exe named file.

The second chain initiates from an RTF document, which when opened executes a html payload – 1[.]html. This payload contains JavaScript tags like the first payload which triggers the ms-msdt: protocol and then goes on to connect to Command & Control Server. Similarly in the third payload, JavaScript tags on a remote HTML payload.

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

05

Feature Rich RAT Spotted in the Wild, WoodyRAT

Tags: Woody RAT, RAT, Follina

A new RAT called Woody RAT was discovered by the threat intelligence team of Malwarebytes. It's been active for the last year. This is an advanced custom RAT designed by threat actors to target Russian continents, especially the Russian aerospace and defense entity known as OAK. The RAT leverages lures in an archive file format and Follina vulnerability.

The prior version of this RAT is supposed to be a document to Russian entities and is delivered, archived into zipping. After the Follina vulnerability came into existence the threat actor started utilizing it with distributed payloads, identified by @MalwareHunterTeam.

The threat actors are using a Microsoft Office document (.docx) inside the zip, to weaponize it with Follina (CVE-2022-30190) Vulnerability to spread and drop the Woody RAT.

Features & capabilities of Woody Rat:

- Woody RAT can, furthermore, execute PowerShell commands and scripts and .NET code received from its C2 server using two DLLs named WoodySharpExecutor and WoodyPowerSession.
- After delivering on a compromised device, the RAT uses process hollowing to inject itself into a suspended Notepad process and deletes itself from the disk as an obfuscation process to evade detection.
- The RAT encrypts C2 communication with the combination of RSA-4096 and AES-CBC to bilk the network-based monitoring.

For IOCs, **refer Appendix 1D**

06

PrivateLoader and Smoke Loader Leveraged by IcedID

Tags: Private Loader, Smoke Loader, IcedID, Djvu, Malware

Researcher at Walmart Global recently identified IcedID (a banking trojan) to be leveraging another malware named Private Loader and Smoke Loader in their campaigns. Private Loader, known for distributing ransomware, stealers, bankers and other malware, was observed to be connected to one of the C2 domains of IcedID loader behind smokeloaders proxies.

This was followed by another interesting observation, wherein the exe file downloaded from one of the C2 domains was actually Djvu ransomware encrypted with the same Cryptor used to encrypt SmokeLoader.

For IOCs, **refer Appendix 1E**

07

A New IoT-based Bot Found Using Mirai like Abilities, Rapperbot

Tags: IoT, Rapperbot, Mirai, Botnet

Actively evolving since June 2022, a bot named "Rapperbot" has been constantly targeting IoT systems to expand its botnet. On analyzing a sample of the same, it is known that the malware family borrows source code from Mirai, another botnet family, however, differentiating the two based on Rapperbot's built-in capability to brute force credentials for SSH servers instead of Telnet, which is done in Mirai.

In their analysis, researchers at Fortinet share various insights regarding the evolving bot, like adding persistence to its tactics, the malware now also contains code for maintaining persistence, that was not covered by Mirai bot, wherein, infected machines once rebooted had SSH connections removed. Primarily targeting Linux distributions, the malware code contains SSH 2.0 client that can connect and brute force any SSH server supporting DH (Diffie-Hellmann) Key Exchange 768-bit or 2048-bit keys.

Post brute forcing SSH for an IoT device, the malware connects back to its C2 server with valid credentials through port 48109 followed by activities like gaining root access, UDP DoS to target DDOS targets.

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

08

Vulnerability in Twitter Code Lets Threat Actor Identify Your PII and Twitter Accounts

Tags: Twitter, Vulnerability, PII Sale

On August 5, 2022, Twitter updated its users of a security incident via a blog, sharing details of what happened and ways to protect its users account from the same. Acknowledging that a bug bounty report in January 2022 reported a vulnerability in Twitter's systems that could potentially tell a threat actor on entering an email address or mobile number, the Twitter account it is connected to, if any.

The bug resulting from an update to source code in June 2021, was identified in July 2022 through various press reports that a threat actor has in fact been leveraging this vulnerability and has brute forced into getting a list of accounts and respective personal identifications, compiled and for sale.

On reviewing the samples shared by threat actor, Twitter claims that the actor had already taken advantage of this vulnerability before it was addressed through the bug report. Suggesting its user's methods to protect their accounts, the team at Twitter recommends the following:

- Do not use publicly known phone numbers and email addresses for your Twitter accounts.
- Enable 2FA ("wo factor Authentication").

09

Cyber Attack on Cisco

Tags: Powersploit, Mimikatz, Google, UNC2447, Lapsus

On May 24, 2022, Cisco identified a potential compromise. The investigation concludes that the victim's personal Google account where credentials saved in, has been compromised by the attacker. The attacker achieved MFA with a series of sophisticated voice phishing attacks. After obtaining the initial access, the attacker enrolled a series of new devices for MFA and authenticated successfully to the Cisco VPN.

Also, the threat actor installed tools like LogMeIn and TeamViewer, offensive security tools such as Cobalt Strike, PowerSploit, Mimikatz, and Impacket, and added their own backdoor accounts and persistence mechanisms. CSIRT and Talos responded to the incident by ensuring that the attacker hadn't gained access to critical internal systems, such as those related to product development, code signing, etc.

Based on the obtained artifacts and TTPs, the investigation team assessed that this attack was conducted by an adversary that has been previously identified as an Initial Access broker (IAB) with ties to both UNC2447 and LAPSUS$.

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

For MITRE Mapping, **refer to Appendix 2A**

10

New Threat Group in Town, Tropical Scorpius

Tags: Threat Group, Tropical Scorpius, Hancitor, Cuba Ransomware

Previously used by the Hancitor Group, Cuba ransomware has been active since December 2019, and now has been observed to be used by another group dubbed as Tropical Scorpius by researchers at Palo Alto Networks. Evolving with time, the ransomware developed its leak site, and till now has claimed 60 organizations publicly as their victims, and undisclosed victims contributing to ransom payments of at least $43.9 million.

The new threat group Tropical Scorpius exploits known vulnerabilities in MS Exchange Servers like ProxyLogon and ProxyShell. In May 2022, a new marketplace named Industrial Spy moved into the ransomware business, and these movements have been correlated to Tropical Scorpius. The Industrial Spy ransomware has been observed to be very similar to Cuba ransomware, right down to the ransom note and contact information on the same.

Another indication of relations between Industrial Spy and Cuba ransomware are that data exfiltrated by Cuba ransomware was posted for sale on the Industrial Spy marketplace. An important tool used by the threat group is ROMCOM, which, though still under active development, has been observed on Virus Total since June 2022.

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

11

Appendix

Appendix

Appendix 1A – Manjusaka framework

Hashes

Maldoc and CS beacon samples
58a212f4c53185993a8667afa0091b1acf6ed5ca4ff8efa8ce7dae784c276927
8e7c4df8264d33e5dc9a9d739ae11a0ee6135f5a4a9e79c354121b69ea901ba6
54830a7c10e9f1f439b7650607659cdbc89d02088e1ab7dd3e2afb93f86d4915

Rust samples
8e9ecd282655f0afbdb6bd562832ae6db108166022eb43ede31c9d7aacbcc0d8
a8b8d237e71d4abe959aff4517863d9f570bba1646ec4e79209ec29dda64552f
3f3eb6fd0e844bc5dad38338b19b10851083d078feb2053ea3fe5e6651331bf2
0b03c0f3c137dacf8b093638b474f7e662f58fef37d82b835887aca2839f529b

C2 binaries
fb5835f42d5611804aaa044150a20b13dcf595d91314ebef8cf6810407d85c64
955e9bbcdf1cb230c5f079a08995f510a3b96224545e04c1b1f9889d57dd33c1

URLs
https[://]39[.]104[.]90[.]45/2WYz
http[://]39[.]104[.]90[.]45/2WYz
http[://]39[.]104[.]90[.]45/IE9CompatViewList.xml
http[://]39[.]104[.]90[.]45/submit.php

IPs
39[.]104[.]90[.]45

Appendix 1B- Lockbit

Hashes 3.0

a512215a000d1b21f92dbef5d8d57a420197d262	Malicious glib-2.0.dll
729eb505c36c08860c4408db7be85d707bdcbf1b	Malicious glib-2.0.dll
10039d5e5ee5710a067c58e76cd8200451e54b55	Malicious glib-2.0.dll
ff01473073c5460d1e544f5b17cd25dadf9da513	Malicious glib-2.0.dll
e35a702db47cb11337f523933acd3bce2f60346d	Encrypted Cobalt Strike payload – c0000015.log
82bd4273fa76f20d51ca514e1070a3369a89313b	Encrypted Cobalt Strike payload – c0000015.log
091b490500b5f827cc8cde41c9a7f68174d11302	Decrypted Cobalt Strike payload – c0000015.log
0815277e12d206c5bbb18fd1ade99bf225ede5db	Encrypted Cobalt Strike payload – c0000013.log
eed31d16d3673199b34b48fb74278df8ec15ae33	Malicious mpclient.dll

Command&Control

Command&Control	
149.28.137[.]7	Cobalt Strike C2
45.32.108[.]54	
139.180.184[.]147	
info.openjdklab[.]xyz	Domain used by the mpclient.dll

Appendix 1C – Follina attacks

Hashes

SHA1 Hash	Description
83fde764f70378b4b0610d87e86faac6dc5bc54b	Word Document
6e9e90431e5e660071b683d121ad887d3726a4a0	7ed97610cdee3c69be2961543ce619485b680572
Linux.Plugin.Lightning.Sshd	HTML Page
8ea0fea3e9787f270a9a23e3335b7b8e35475b06	Cobalt Strike Loader
8b095d4f5b1ef62b40507e6155a55214243f2c85	RTF Document
1c52a8bab1e5a107837c2d9abab1c73d571dc15d	RTF Document
b0b952334f0d0195b06faed532170263f7fad6c2	HTML Page
da80a38090ef8cb52e91e639ea267c4f24bf3a21	PowerShell Trojan
64e5715d590c54a7c06baceef19e84ef672bc257	PowerShell Trojan
3c7674214e21cc4ec6a92555a1e6d1ad5c7ed36f	PowerShell (Invoke-Mimikatz)
70dcbbcc20addef04eae7bf66c1545a935005c69	HTML Page
82b0beb6fff9a90dc40b300ebf1b0ec4977ba8ad	Unknown Backdoor

Network
files.attend-doha-expo[.]com
5.206[.]224.233
www[.]telecomly[.]info
seller-notification[.]live
65.20[.]75.158
t1bet[.]net
tibetyouthcongress[.]com
45.77[.]45.222:110

Appendix 1D- Woody RAT

Woody Rat Hashes
982ec24b5599373b65d7fec3b7b66e6afff4872847791cf3c5688f47bfcb8bf0
66378c18e9da070629a2dbbf39e5277e539e043b2b912cc3fed0209c48215d0b
b65bc098b475996eaabbb02bb5fee19a18c6ff2eee0062353aff696356e73b7a
43b15071268f757027cf27dd94675fdd8e771cdcd77df6d2530cb8e218acc2ce
408f314b0a76a0d41c99db0cb957d10ea8367700c757b0160ea925d6d7b5dd8e
0588c52582aad248cf0c43aa44a33980e3485f0621dba30445d8da45bba4f834
5c5020ee0f7a5b78a6da74a3f58710cba62f727959f8ece795b0f47828e33e80
3ba32825177d7c2aac957ff1fc5e78b64279aeb748790bc90634e792541de8d3
9bc071fb6a1d9e72c50aec88b4317c3eb7c0f5ff5906b00aa00d9e720cbc828d

C2s
kurmakata.duckdns[.]org
microsoft-ru-data[.]ru
194.36.189.179
microsoft-telemetry[.]ru
oakrussia[.]ru

Appendix 1E – IcedID, SmokeLoader & Djvu Ransomware

Network IOCs
rgyui.top
allejee.com
194.87.31.137
2.58.28.60
host-file-host6.com
host-host-file8.com
64.52.80.224 - Raccoon Stealer
deficulintersun.com - IcedID
acacaca.org - Djvu Ransomware

Appendix 1F – RapperBot

Hashes
92ae77e9dd22e7680123bb230ce43ef602998e6a1c6756d9e2ce5822a09b37b4
a31f4caa0be9e588056c92fd69c8ac970ebc7e85a68615b1d9407a954d4df45d
e8d06ac196c7852ff71c150b2081150be9996ff670550717127db8ab855175a8
23a415d0ec6d3131f1d537836d3c0449097e98167b18fbdbf2efca789748818a
c83f318339e9c4072010b625d876558d14eaa0028339db9edf12bbcafe6828bb
05c78eaf32af9647f178dff981e6e4e43b1579d95ccd4f1c2f1436dbfa0727ad
88bbb772b8731296822646735aacbfb53014fbb7f90227b44523d7577e0a7ce6
e8f1e8ec6b94ea54488d5f714e71e51d58dcdfe4be3827c55970d6f3b06edf73
23256f231f3d91b0136b44d649b924552607a29b43a195024dbe6cde5b4a28ad
77b2e5fb5b72493bde35a6b29a66e6250b6a5a0c9b9c5653957f64a12c793cd5
dcdeedee4736ec528d1a30a585ec4a1a4f3462d6d25b71f6c1a4fef7f641e7ae
ebb860512a55c1cdc8be1399eec44c4481aedb418f15dbda4612e6d38e9b9010
9d234e975e4df539a217d1c4386822be1f56cea35f7dd2aa606ae4995894da42
1975851c916587e057fa5862884cbac3fa1e80881ddd062392486f5390c86865
8380321c1bd250424a0a167e0f31951161lf73b53736895a8d3a2ad58ffcd5d5
f5ff9d1261af176d7ff1ef91aa8c892c70b40caa02c17a25de22539e9d0cdd26
2298071b6ba7baa5393be064876efcdbd9217c212e0c764ba62a6f0ffc83cc5a
2479932a6690f070fa344e5222e3fbb6ad9c880294d5b822d7a3ec27f1b8b8d5
1d5e6624a2ce55616ef078a72f25c9d71a3dbc0175522c0d8e07233115824f96
746106403a98aea357b80f17910b641db9c4fedbb3968e75d836e8b1d5712a62
ddf5aff0485f395c7e6c3de868b15212129962b4b9c8040bef6679ad880e3f31

Hashes
e56edaa1e06403757e6e2362383d41db4e4453aafda144bb36080a1f1b899a02
55ff25b090dc1b380d8ca152428ba28ec14e9ef13a48b3fd162e965244b0d39b
8e9f87bb25ff83e4ad970366bba47afb838028f7028ea3a7c73c4d08906ec102
d86d158778a90f6633b41a10e169b25e3cb1eb35b369a9168ec64b2d8b3cbeec
ff09cf7dfd1dc1466815d4df098065510eec504099ebb02b830309067031fe04

Download URLs
hxxp://31[.]44[.]185[.]235/x86
hxxp://31[.]44[.]185[.]235/mips
hxxp://31[.]44[.]185[.]235/arm7
hxxp://2[.]58[.]149[.]116/arm
hxxp://2[.]58[.]149[.]116/spc
hxxp://2[.]58[.]149[.]116/mips
hxxp://2[.]58[.]149[.]116/x86_64
hxxp://2[.]58[.]149[.]116/ssh/arm7
hxxp://2[.]58[.]149[.]116/ssh/mips
hxxp://2[.]58[.]149[.]116/ssh/x86
hxxp://2[.]58[.]149[.]116/ssh/spc
hxxp://194[.]31[.]98[.]244/ssh/new/spc
hxxp://194[.]31[.]98[.]244/ssh/new/x86
hxxp://194[.]31[.]98[.]244/ssh/new/mips
hxxp://194[.]31[.]98[.]244/ssh/new/arm7
hxxp://194[.]31[.]98[.]244/ssh/new/arm
hxxp://194[.]31[.]98[.]244/ssh/new/x86
hxxp://194[.]31[.]98[.]244/ssh/new/mips
hxxp://194[.]31[.]98[.]244/ssh/new/arm7
hxxp://194[.]31[.]98[.]244/ssh/new/arm
hxxp://185[.]225[.]73[.]196/ssh/new/arm
hxxp://185[.]225[.]73[.]196/ssh/new/arm7
hxxp://185[.]225[.]73[.]196/ssh/new/mips
hxxp//185[.]225[.]73[.]196/ssh/new/x86

C2 IPs
31[.]44[.]185[.]235
2[.]58[.]149[.]116
194[.]31[.]98[.]244
185[.]225[.]73[.]196

Appendix 1G – Cyber Attack on Cisco

Hashes (SHA256)
184a2570d71eedc3c77b63fd9d2a066cd025d20ceef0f75d428c6f7e5c6965f3
2fc5bf9edcfa19d48e235315e8f571638c99a1220be867e24f3965328fe94a03
542c9da985633d027317e9a226ee70b4f0742dcbc59dfd2d4e59977bb870058d
61176a5756c7b953bc31e5a53580d640629980a344aa5ff147a20fb7d770b610
753952aed395ea845c52e3037f19738cfc9a415070515de277e1a1baeff20647
8df89eef51cdf43b2a992ade6ad998b267ebb5e61305aeb765e4232e66eaf79a
8e5733484982d0833abbd9c73a05a667ec2d9d005bbf517b1c8cd4b1daf57190
99be6e7e31f0a1d7eebd1e45ac3b9398384c1f0fa594565137abb14dc28c8a7f
bb62138d173de997b36e9b07c20b2ca13ea15e9e6cd75ea0e8162e0d3ded83b7
eb3452c64970f805f1448b78cd3c05d851d758421896edd5dfbe68e08e783d18

IP Addresses
104.131.30[.]201
108.191.224[.]47
131.150.216[.]118
134.209.88[.]140
138.68.227[.]71
139.177.192[.]145
139.60.160[.]20
139.60.161[.]99
143.198.110[.]248

IP Addresses
143.198.131[.]210
161.35.137[.]163
162.33.177[.]27
162.33.178[.]244
162.33.179[.]17
165.227.219[.]211
165.227.23[.]218
165.232.154[.]73
166.205.190[.]23
167.99.160[.]91
172.56.42[.]39
172.58.220[.]52
172.58.239[.]34
174.205.239[.]164
176.59.109[.]115
178.128.171[.]206
185.220.100[.]244
185.220.101[.]10
185.220.101[.]13
185.220.101[.]15
185.220.101[.]16

IP Addresses
185.220.101[.]2
185.220.101[.]20
185.220.101[.]34
185.220.101[.]45
185.220.101[.]6
185.220.101[.]65
185.220.101[.]73
185.220.101[.]79
185.220.102[.]242
185.220.102[.]250
192.241.133[.]130
194.165.16[.]98
195.149.87[.]136
24.6.144[.]43
45.145.67[.]170
45.227.255[.]215
45.32.141[.]138
45.32.228[.]189
45.32.228[.]190
45.55.36[.]143
45.61.136[.]207
45.61.136[.]5
45.61.136[.]83

IP Addresses
46.161.27[.]117
5.165.200[.]7
52.154.0[.]241
64.227.0[.]177
64.4.238[.]56
65.188.102[.]43
66.42.97[.]210
67.171.114[.]251
68.183.200[.]63
68.46.232[.]60
73.153.192[.]98
74.119.194[.]203
74.119.194[.]4
76.22.236[.]142
82.116.32[.]77
87.251.67[.]41
94.142.241[.]194

Domains
cisco-help[.]cf
cisco-helpdesk[.]cf
ciscovpn1[.]com
ciscovpn2[.]com
ciscovpn3[.]com
devcisco[.]com
devciscoprograms[.]com
helpzonecisco[.]com
kazaboldu[.]net
mycisco[.]cf
mycisco[.]gq
mycisco-helpdesk[.]ml
primecisco[.]com
pwresetcisco[.]com

Email Addresses
costacancordia[@]protonmail[.]com

Appendix 1H – Tropical Scorpius & Cuba Ransomware

Hashes	
07905de4b4be02665e280a56678c7de67652aee318487a44055700396d37ecd0	Driver Dropper
af6561ad848aa1ba53c62a323de230b18cfd30d8795d4af36bf1ce6c28e3fd4e	
24e018c8614c70c940c3b5fa8783cb2f67cb13f08112430a4d10013e0a324eaa	
ab5a3bbad1c4298bc287d0ac8c27790d68608393822da2365556ba99d52c5dfb	ZeroLogon Hacktool
6866e82d0f6f6d8cf5a43d02ad523f377bb0b374d644d2f536ec7ec18fdaf576	
3febf726ffb4f4a4186571d05359d2851e52d5612c5818b2b167160d367f722c	
3a8b7c1fe9bd9451c0a51e4122605efc98e7e4e13ed117139a13e4749e211ed0	
36bc32becf287402bf0e9c918de22d886a74c501a33aa08dcb9be2f222fa6e24	
1450f7c85bfec4f5ba97bcec4249ae234158a0bf9a63310e3801a00d30d9abcc	
0a3517d8d382a0a45334009f71e48114d395a22483b01f171f2c3d4a9cfdbfbf	Cuba Ransomware
0eff3e8fd31f553c45ab82cc5d88d0105626d0597afa5897e78ee5a7e34f71b3	
a4665231bad14a2ac9f2e20a6385e1477c299d97768048cb3e9df6b45ae54eb8	Privilege Escalation Tool
cfe7b462a8224b2fbf2b246f05973662bdabc2c4e8f4728c9a1b977fac010c15	KerberCache Hacktool

Hashes	
B5978cf7d0c275d09bedf09f07667e139ad7fed8f9e47742e08c914c5cf44a53	ROMCOM RAT
324ccd4bf70a66cc14b1c3746162b908a688b2b124ad9db029e5bd42197cfe99	
3496e4861db584cc3239777e137f4022408fb6a7c63152c57e019cf610c8276e	

Infrastructure
CombinedResidency[.]org
optasko[.]com

Appendix 2A – Cyber Attack on Cisco

MITRE ATT&CK MAPPING previously described TTPs that were observed in this attack are listed below based on the phase of the attack in which it occurred

Initial Access

- ATT&CK Technique : Phishing (T1566)
- ATT&CK Technique : Valid Accounts (T1078)

Execution

- ATT&CK Technique : System Services: Service Execution (T1569.002)

Persistence

- ATT&CK Technique : Create Account: Local Account (T1136.001)
- ATT&CK Technique : Account Manipulation: Device Registration (T1098.005)

Privilege Escalation

ATT&CK Technique : Event Triggered Execution: Image File Execution Options Injection (T1546.012)

Defense Evasion

- ATT&CK Technique : Indicator Removal on Host (T1070)
- ATT&CK Technique : Indicator Removal on Host: Clear Windows Event Logs (T1070.001)
- ATT&CK Technique : Masquerading: Match Legitimate Name or Location (T1036.005)
- ATT&CK Technique : Impair Defenses: Disable or Modify System Firewall (T1562.004)
- ATT&CK Technique : Modify Registry (T1112)

Credential Access

- ATT&CK Technique : OS Credential Dumping: LSASS Memory (T1003.001)
- ATT&CK Technique : OS Credential Dumping: Security Account Manager (T1003.002)
- ATT&CK Technique : OS Credential Dumping: NTDS (T1003.003)
- ATT&CK Technique : Multi-Factor Authentication Request Generation (T1621)

Lateral Movement

ATT&CK Technique : Remote Services (T1021)

Discovery

ATT&CK Technique : Query Registry (T1012)

Command and Control

- ATT&CK Technique : Application Layer Protocol: Web Protocols (T1071.001)
- ATT&CK Technique : Remote Access Software (T1219)
- ATT&CK Technique: Encrypted Channel: Asymmetric Cryptography (T1573.002)
- ATT&CK Technique : Proxy: Multi-hop Proxy (T1090.003)

Exfiltration

ATT&CK Technique : Exfiltration Over Alternative Protocol (T1048)

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