Payatu

March 2023

Cyber Threat Intelligence Report

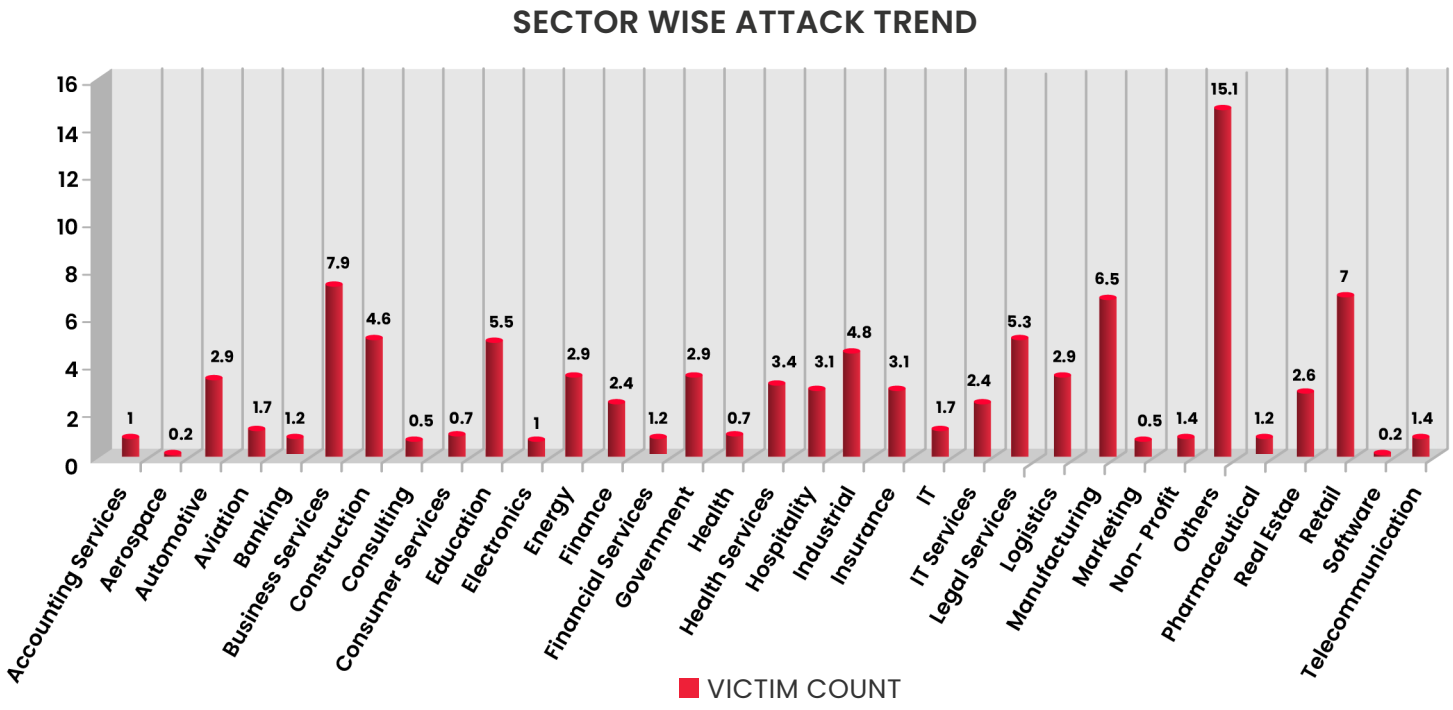
Payatu Security Consulting Pvt. Ltd.

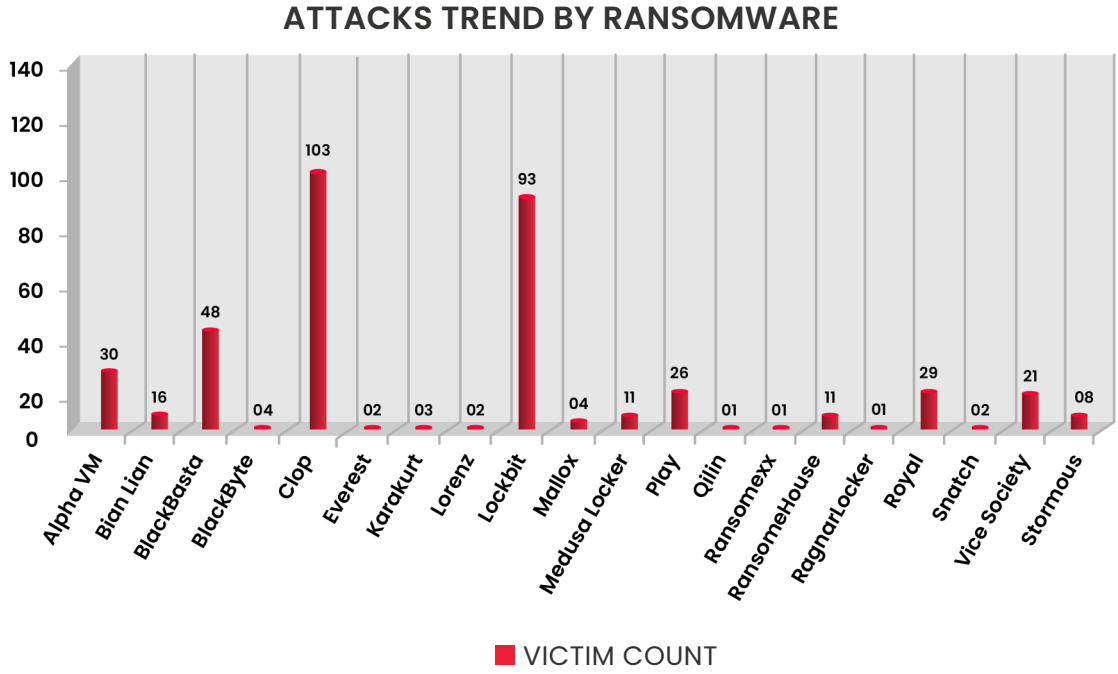
Table of Contents

01

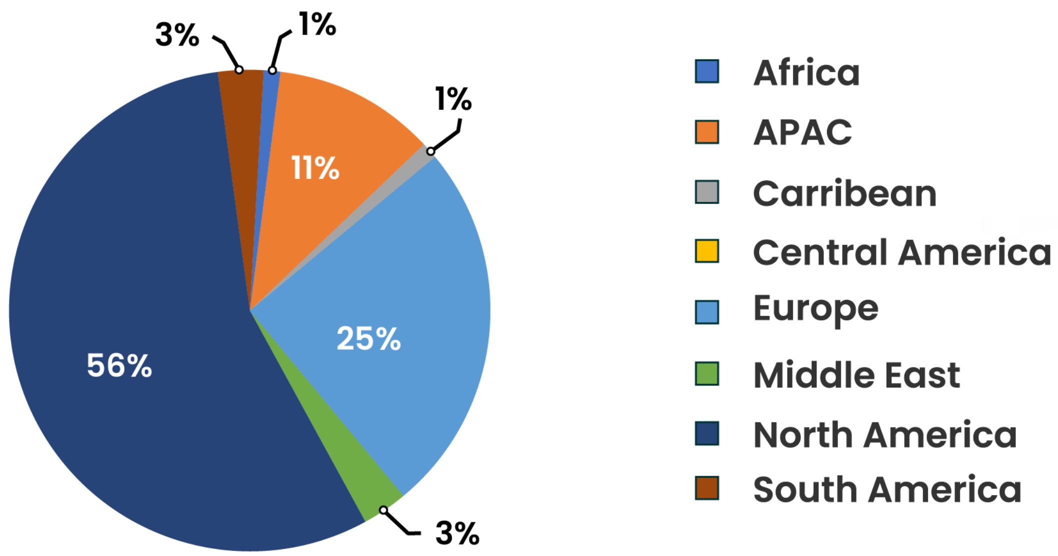
Ransomware Statistics

- Clop Ransomware published 103 new victims, which include Axis Bank, Hatch Bank (US), Rubrik, Pluralsight, Hitachi Energy, Invest Quebec, PG (Procter & Gamble) Co. etc.
- Sun Pharmaceutical Ltd. Compromised by AlphVM ransomware.
- Piramal Conglomerate compromised by Lockbit3 ransomware.
- Increase in ransomware attacks in India by 4 times since December 2022

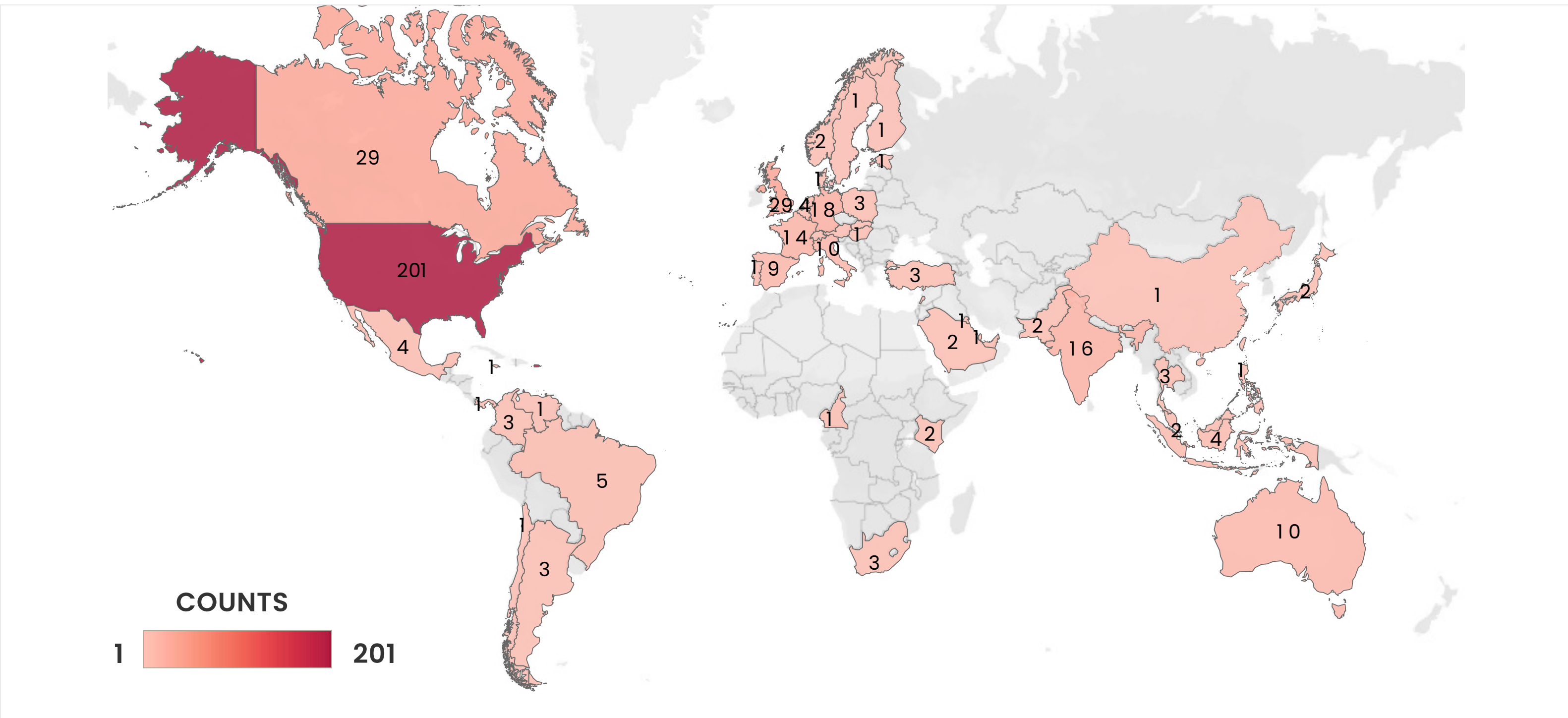




REGIONWISE ATTACK



COUNTRY-WISE ATTACK TREND - 416



02

Sharp Panda Operations Targeting Government Entities in Southeast Asia

Tags: Government, Southeast Asia, Sharp Panda

Previously targeting sectors like defense, healthcare, ICT in Southeast Asia, Sharp Panda is a state-sponsored cyber espionage group of Chinese origin. In its latest campaign, the group has been using Soul malware/framework, specifically the Soulsearcher loader as a payload. The initial access vector involves government-themed, attachments-based spear phishing email to the targeted networks. The attachments which are usually Word documents, leverage a remote template to download and run malicious RTF documents, weaponized with RoyalRoad kit.

RoyalRoad kit creates scheduled tasks that execute and download **5.t** downloader, a custom DLL downloader, along with a second-stage loader responsible for downloading the final payload, i.e. Soulsearcher loader. The soulsearcher loader executes the Soul backdoor that communicates to a geo-fenced C&C server. A geo-fenced server responds to requests from a specific geographical location, in this case, Southeast Asian countries like Vietnam, Thailand, and Indonesia. Soul backdoors unique feature of "radio silence" that allows the main module to lay low for a time specified by the threat actor; that is, there is no communication to the C&C server for the duration. This feature makes it difficult to detect malware in the environment if the file-hash is relatively new and not monitored by endpoint security products.

For a detailed report, refer to Checkpoint Research.

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

03

CISA Shares Advisories for Eight Industrial Control Systems (ICS)

Tags: ICS, Energy, Manufacturing, CISA, Siemens, Hitachi, Delta Electronics

On March 21, 2023, CISA shared eight Industrial Control System (ICS) advisories, comprising security issues, exploits and vulnerabilities surrounding 3 products of Siemens and 1 product each for Hitachi Energy, Keysight Technologies, Delta Electronics, Rockwell and VISAM. The products/ systems are used in multiple sectors, some of which include, government, communications, energy, and critical manufacturing.

Most of the vulnerabilities lie in medium and high severity levels, while two vulnerabilities, CVE-2023-1133 in Delta Electronics' infrasuite devices, and CVE-2023-27855 in Rockwell Automation's ThinManager are marked as critical severity levels.

CVE-2023-1133 is deserialization of untrusted data due to default listening of device-status service, allowing an unauthenticated attacker to remotely execute arbitrary code. Other vulnerabilities in Delta Electronics' products include improper access control, path traversal, improper authentication, etc.

CVE-2023-27855 is a path traversal vulnerability, wherein an unauthenticated remote attacker could upload arbitrary files to any directory. Other vulnerabilities include path traversal, heap-based buffer overflow, etc.

A complete list of vulnerabilities is mentioned in **Appendix 1B.**

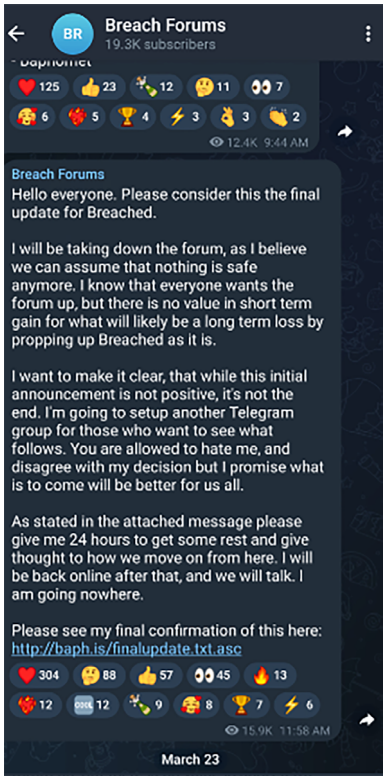
04

Breached Forum Administrator Arrested, New Admin Shuts Down the Forum for Now

Tags: Darkweb, Breached Forum

On March 15, 2023, government agencies in the United States of America arrested a 21-year-old threat actor connected to Breached Forum, a dark web forum similar to RaidForums that was used by various hackers as a forum to sell, purchase, discuss and share leaked or hacked data. Going by the alias “pompompurin”, the threat actor was the administrator of Breached Forum.

In the given circumstances, another administrator code named “Baphomet” shared an update on the group’s Telegram channel, announcing that the forum will be temporarily shut down, as the forum might be compromised. Since then, the forum has not been accessible.



The implications of the forum going down are that, on one hand this results in lower data propagation as breached, which basically inherited most of its capabilities from RaidForums, was one of the preferred spaces for threat actors selling stolen databases; while on the other hand it will be difficult to monitor activities of threat actors as a central source is out of line.

Multiple Telegram channels, separate forums have been set up after RaidForums was seized. Similar action may lead to more diversification of threat actor leak sources.

05

Winter Vivern Targets Government Entities in a Global Espionage

Tags: Government, Telecommunications, India, Lithuania, Slovakia

First observed in 2021 by DomainTools, Winter Vivern is a pro-Russian APT group, attributed to the Command & Control Server domain. Recently observed by SentinelOne, the group has been targeting Government entities of India, Lithuania, Slovakia, Vatican, etc. using phishing emails. Other specific targets include private telecommunications providers.

The initial techniques used by the group revolve around phishing, either by using malicious documents, or by mimicking government sites. Fake government sites that contain login options are used to steal credentials. In case of malicious documents, XLS files containing macros which call PowerShell invoke-expression, is then executed to beacon a malicious destination.

Winter Vivern is known for its resourcefulness and not using specific malware family always. In recent encounters the malware family being used is dubbed as APERETIF, which is PE32 executables written in Visual C++ with PowerShell scripting. It automates victim details, maintaining access, to beacon to a threat actor-controlled domain. Other intrusion techniques include exploiting vulnerabilities in public-facing applications of specific targets.

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

06

Australian Insurance Giant Latitude Financial Suffers Massive Data Breach

Tags: Insurance, Financial Services, Australia, New Zealand

On March 16, 2023, Latitude Financial, the largest non-bank lender of consumer credit in Australia, informed its customers of some suspicious activity on its internal network, which turned out to be a malicious cyber-attack. This resulted in data leak of approximately 14 million customer records. The data leaked is of Personal Identifiable Information (PII) nature, comprising copies of driver licenses and driver license numbers, copies of passports and passport numbers, and medicare details.

Customers of the company that have been impacted by the breach primarily belong to Australia and New Zealand, and this data includes existing as well as old customers. The threat actor breached the internal systems of the company, gained login credentials for a Latitude employee, accessed two service providers/vendors using these credentials, and stole data from the access portals for the vendors.

07

Fake ChatGPT Chrome Extensions Targeting Facebook Cookies and Hijacking Accounts

Tags: Artificial Intelligence, ChatGPT, Facebook, Chrome Store

Researchers at Guard.io uncovered a malicious ChatGPT campaign targeting Facebook using Chrome Extensions. Active since March 3, 2023, **9000 victims** of the campaign who have installed the extension.

The first variant of the campaign impersonated as “Quick Access to ChatGPT” providing an extension icon to query anything to ChatGPT. Once allowed, it is capable of sending a request to any other services on behalf of the browser, like Facebook. The extension then harvests the details like token, client IP, tokenEQs which connect with Facebook, hence accessing session cookies. This is followed by multiple automated processes capable of accessing other Meta accounts like WhatsApp and Instagram.

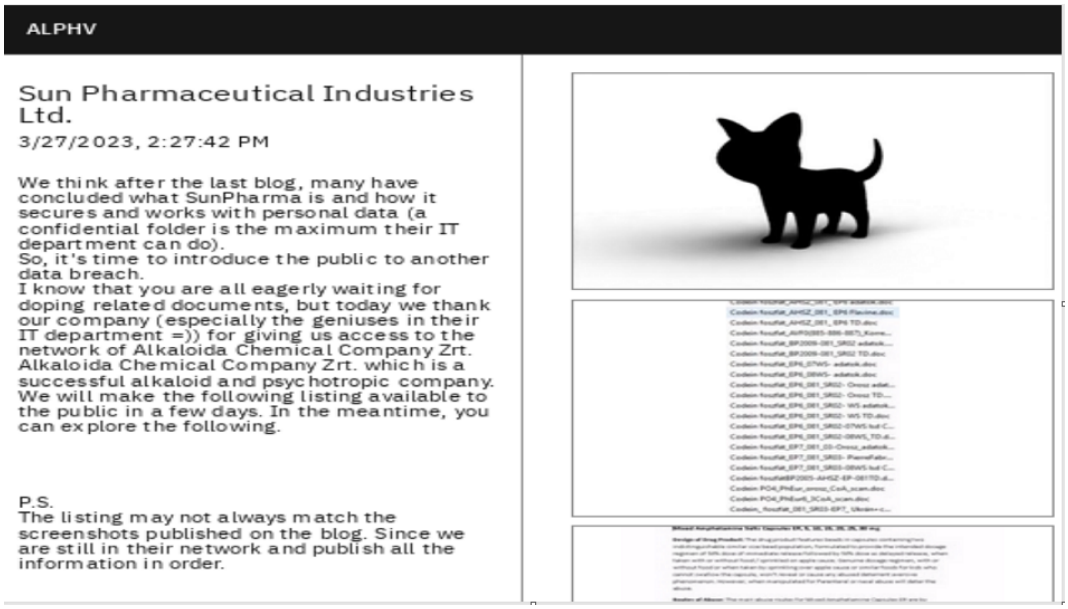
Another variant recently identified, impersonates as “ChatGPT for Google”, and is published by chatgpt4google.com. This extension too performs Cookie-Hijacking specifically for Facebook. The hijacked accounts are renamed to “Lily Collins” and harvested accounts are used to promote posts around the ISIS propaganda.

08

Sun Pharmaceuticals Hit by Alphv Ransomware, 17 TB of Data Leaked

Tags: Pharmaceutical, Health services, Alphv

Alphv Ransomware group announced Sun Pharmaceuticals, India's leading pharmaceutical company as its latest victim on March 24, 2023. This resulted in exposure of a massive 17 TB of data, out of which few samples have been shared by the group. The data involved in this breach contains Personal Identifiable Information (PII) and passport snapshots of around 1500 employees belonging to India, the US, Italy, and few other countries of Europe.



Source: vqifktlreqpudvulhbzmc5gocbeawl67uvs2pttswemdorbnhaddohyd[.]onion

Note: It is not advisable to access the link. Pursue with caution.

As per the sample attachments and blogs of the group, data involved dates back to 2006. The samples contain multiple customer documents and research and development documents with a Hungarian company, "Alkaloida Chemical Company Zrt", which the group claims to have access of, as a result of this breach. The companies are involved in developing successful alkaloid and psychotropic drugs (drugs that assist in dealing with issues like depression, anxiety, etc.)

Sun Pharmaceutical Industries Limited
Sun House, Plot No. 201 B/1,
Western Express Highway, Goregaon (E),
Mumbai – 400 063, Maharashtra, INDIA.
Tel. : (91-22) 4324 4324
Fax : (91-22) 4324 4343
Website: www.sunpharma.com
CIN: L24230GJ1993PLC019050

March 2, 2023

National Stock Exchange of India Ltd.,
Exchange Plaza, 5th Floor,
Plot No. C/1, G Block,
Bandra Kurla Complex,
Bandra (East), Mumbai – 400 051.

Scrip Symbol: SUNPHARMA

BSE Limited,
Market Operations Dept.
P. J. Towers,
Dalal Street,
Mumbai - 400 001.

Stock Code: 524715

Dear Sirs,

Sub: Intimation of IT Security Incident

Dear Sir / Madam,

This is to inform that an information security incident has occurred at the Company and the impacted IT assets have been isolated. The incident has not impacted our core systems and operations. The Company is investigating the matter and appropriate containment and remediation actions are being taken in a controlled manner to address the incident.

This is for your information and dissemination.

Thanking you,

For Sun Pharmaceutical Industries Limited

Source: bseindia

The company in its exchange filing to BSE has informed BSE and its customers of the cyber incident on March 2, 2023. While the threat group continues to claim persistent access to the network, the company has proceeded to isolate networks where data breach was identified. There has been a major business impact on the company, with reduced revenues and stock market losses.

09

Spyware Exploiting Zero-days in iOS and Android Devices

Tags: Android, iOS, Spyware

In a recent analysis by Google Threat Analysis Group (TAG), researchers have uncovered malicious campaigns involved in inter-governmental attacks, information operation (spyware), and financial motivated attacks. These campaigns are propagated through shortened bit URLs (bit[.]ly) which can exploit zero-days and n-days exploits in Android, Chrome and iOS devices.

Sent over SMS, the bit[.]ly links redirect to pages hosting exploits for above device categories and then redirect the victims to legitimate websites. Few cases observed in Italy, Malaysia, Kazakhstan have seen similarity in this modus operandi (MO). iOS devices were actively exploited using CVE-2022-42856, which is a remote code execution (RCE). Within its JIT compiler, CVE-2021-30900, a privilege escalation and sandbox escape vulnerability are also being actively exploited.

Android devices are being targeted using CVE-2022-3723, CVE-2022-4135, CVE-2022-38181, which are type confusion, sandbox bypass, and privilege escalation vulnerabilities respectively. Samsung devices, on the other hand, are specifically being targeted using vulnerabilities like CVE-2022-22706 in its default Internet browser.

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

10

Massive Supply Chain Attack Hits 3CX Systems and its Clients

Tags: Supply Chain Attack, Telecommunications

3CX Systems is a pioneer in Business Communication Solutions and Software, used by major companies of the world for managing their customer care solutions (Softphone, SMS, Chatbox Assistance). The client base of 3CX includes companies from the automobile sector such as Mercedes Benz, BMW, Toyota, Honda; companies from the food & beverages sector such as McDonalds, Coca Cola, Pizza Hut; companies from the healthcare sector such as NHS (UK); and IT companies like ClearSwift.

A legitimate signed file that is used by 3CX clients as a part of its desktop app has been injected with malicious code resulting in a Supply Chain attack. The Windows Electron-based clients of 3CX desktop app versioned: 18.12.407, 18.12.416 and Electron Mac app versioned: 18.11.1213, 18.12.402, 18.12.407, 18.12.416 are affected.

As of now, 3CX has taken down the domains which were contacted by malicious file. The GitHub repository where the domains were listed has also been taken down. A revised version of the application is in development and soon will be shared. Meanwhile, customers should uninstall 3CX desktop app and use the PWA app for business continuity.

For further details, refer to 3CX Systems.

10

Appendix

Appendix 1A – Sharp Panda

C&C servers
45.76.190[.]210
45.197.132[.]68
45.197.133[.]23
103.78.242[.]11
103.159.132[.]96
103.173.154[.]168
103.213.247[.]48
139.180.137[.]73
139.180.138[.]49
152.32.243[.]17
office.oiqezet[.]com

Hashes

Phishing documents
32a0f6276fea9fe5ee2ffda461494a24a5b1f163a300bc8edd3b33c9c6cc2d17
ca7f297dc04acad2fab04d5dc2de9475aed4186805f6c237c10b8f56b-384cf30
341dee709285286bc5ba94d14d1bce8a6416cb93a054bd183b501552a17ef314
9d628750295f5cde72f16da02c430b5476f6f47360d008911891fdb5b14a1a01
811a020b0f0bb31494f7fbe21893594cd44d90f77fcd1f257925c4ac5fabed43
b023e2b398d552aacb2233a6e08b4734c205ab6abf5382ec31e6d5aa7c-71c1cb

External template (RoyalRoad RTF)
81d9e75d279a953789cbbe9ae62ce0ed625b61d123fef8ffe49323a04fecdb3f
12c1a4c6406ff378e8673a20784c21fb997180cd333f4ef96ed4873530baa8d3
f2779c63373e33fdbd001f336df36b01b0360cd6787c1cd29a6524cc7bcf1ffb
7a7e519f82af8091b9ddd14e765357e8900522d422606aefda949270b9b-f1a04
4747e6a62fee668593ceebf62f441032f7999e00a0dfd758ea5105c1feb72225
3541f3d15698711d022541fb222a157196b5c21be4f01c5645c6a161813e85eb

5.t Downloader
0f9f85d41da21781933e33dddcc5f516c5ec07cc5b4cff53ba388467bc6ac3fd
17f4a21e0e8c0ce958baf34e45a8b9481819b9b739f3e48c6ba9a6633cf-85b0e
f8622a502209c18055a308022629432d82f823dd449abd9b-17c61e363a890828
1a15a35065ec7c2217ca6a4354877e6a1de610861311174984232ba5ff749114
065d399f6e84560e9c82831f9f2a2a43a7d853a27e922cc81d3bc5fcd1adfc56
1e18314390302cd7181b710a03a456de821ad85334acfb55f535d311dd6b3d65
c4500ad141c595d83f8dba52fa7a1456959fb0bc2ee6b0d0f687336f51e1c14e
390e6820b2cc173cfd07bcebd67197c595f4705cda7489f4bc44c933ddcf-8de6

SoulSearcher
d1a6c383de655f96e53812ee1dec87dd51992c-4be28471e44d7dd558585312e0

Soul Backdoor
df5fe7ec6ecca27d3affc901cb06b27dc63de9ea8c97b87b-c899a79eca951d60

Appendix 1B – ICS vulnerabilities

Vulnerability	Advisory
CVE-2023-1399	ICSA-23-080-01 Keysight N6854A Geolocation Server and N6841A RF Sensor
CVE-2023-1133	ICSA-23-080-02 Delta Electronics InfraSuite Device Master
CVE-2023-1139	
CVE-2023-1145	
CVE-2023-1138	
CVE-2023-1144	
CVE-2023-1137	
CVE-2023-1143	
CVE-2023-1134	
CVE-2023-1142	
CVE-2023-1136	
CVE-2023-1141	
CVE-2023-1135	
CVE-2023-1140	

Vulnerability	Advisory
CVE-2022-32469	ICSA-23-080-03 Siemens RUGGEDCOM APE1808 Product Family
CVE-2022-32470	
CVE-2022-32471	
CVE-2022-32475	
CVE-2022-32477	
CVE-2022-32953	
CVE-2022-32954	
CVE-2022-38767	ICSA-23-080-04 Siemens RADIUS Client of SIPROTEC 5 Devices
CVE-2022-38767	ICSA-23-080-05 VISAM VBASE Automation Base
CVE-2022-41696	
CVE-2022-43512	
CVE-2022-45121	
CVE-2022-45468	
CVE-2022-45876	
CVE-2022-46286	
CVE-2022-46300	
CVE-2023-27855	ICSA-23-080-06 Rockwell Automation ThinManager
CVE-2023-27856	
CVE-2023-27857	

Vulnerability	Advisory
CVE-2018-12886	ICSA-23-080-07 Siemens SCALANCE Third-Party
CVE-2018-25032	
CVE-2021-42373	
CVE-2021-42374	
CVE-2021-42375	
CVE-2021-42376	
CVE-2021-42377	
CVE-2021-42378	
CVE-2021-42379	
CVE-2021-42380	
CVE-2021-42381	
CVE-2021-42382	
CVE-2021-42383	
CVE-2021-42384	
CVE-2021-42385	
CVE-2021-42386	
CVE-2022-23395	
CVE-2021-35534	ICSA-21-343-01 Hitachi Energy GMS600, PWC600, and Relion (Update A)

Appendix 1C – Winter Vivern

Domains
bugiplaysec[.]com
marakanas[.]com
ocs-romastassec[.]com
ocspdep[.]com
security-ocsp[.]com
troadsecow[.]com
hxxps://applesaltbeauty[.]com/wordpress/wp-includes/widgets/class-wp/521734i
hxxps://marakanas[.]com/Kkdn7862Jj6h2oDASGmpqU4Qq4q4.php
hxxps://natply[.]com/wordpress/wp-includes/fonts/ch/097214o
hxxps://ocs-romastassec[.]com/goog_comredira3cf7ed34f8.php

IP
176.97.66[.]57
179.43.187[.]175
179.43.187[.]207
195.54.170[.]26
80.79.124[.]135

SHA-1
0fe3fe479885dc4d9322b06667054f233f343e20
83f00ee38950436527499769db5c7ecb74a9ea41
a19d46251636fb46a013c7b52361b7340126ab27
a574c5d692b86c6c3ee710af69fccbb908fe1bb8
c7fa6727fe029c3eaa6d9d8bd860291d7e6e3dd0
f39b260a9209013d9559173f12fbc2bd5332c52a

Appendix 1D – Spyware targeting iOS, Android devices

Domains
hxxps[://]cdn.cutlink[.]site/p/uu6ekt - landing page
hxxps[://]api.cutlink[.]site/api/s/N0NBL8/ - Android exploit chain
hxxps[://]api.cutlink[.]site/api/s/3PU970/ - iOS exploit chain
hxxps[://]imjustarandomsite.3utilities[.]com - exploit delivery server
www[.]sufficeconfigure[.]com - landing page and exploit delivery
www[.]anglesyen[.]org - malware C2

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