Payatu

April 2023

Cyber Threat Intelligence Report

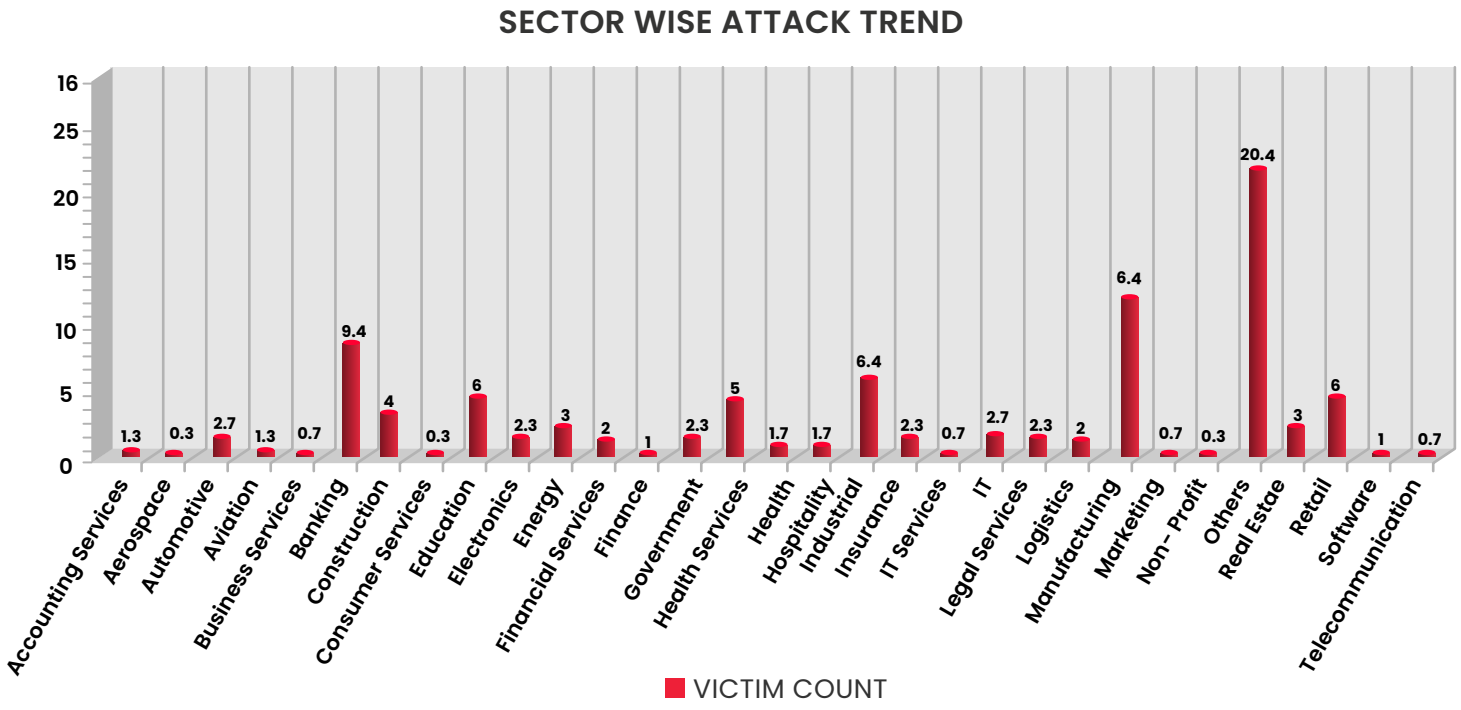
Payatu Security Consulting Pvt. Ltd.

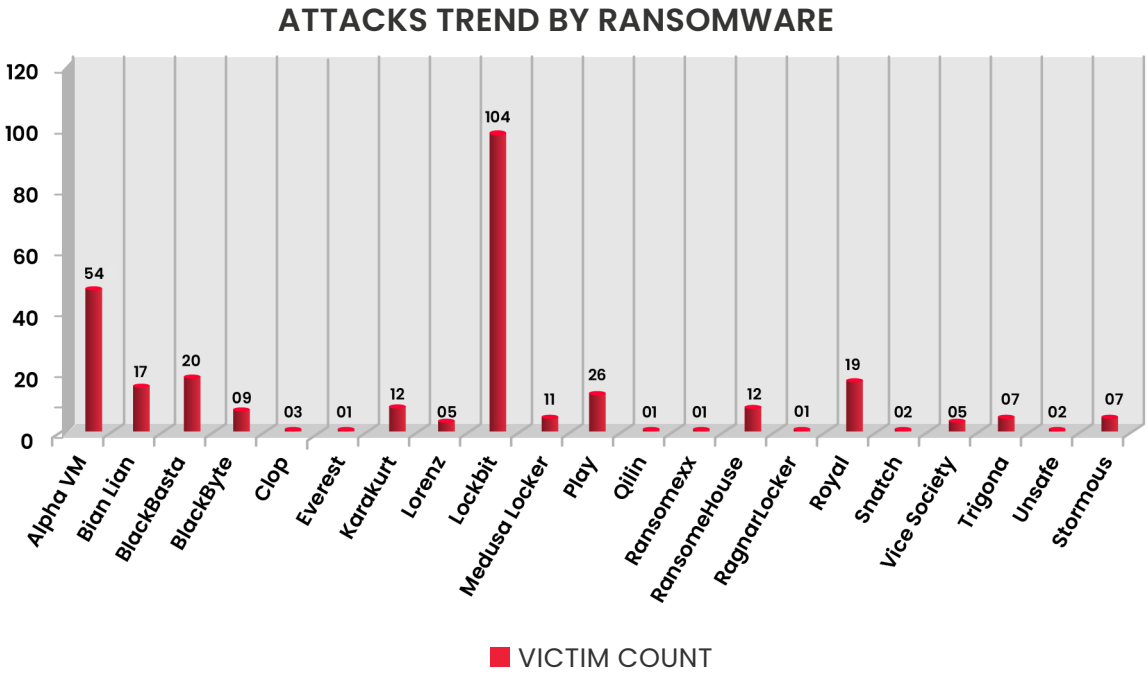
Table of Contents

01

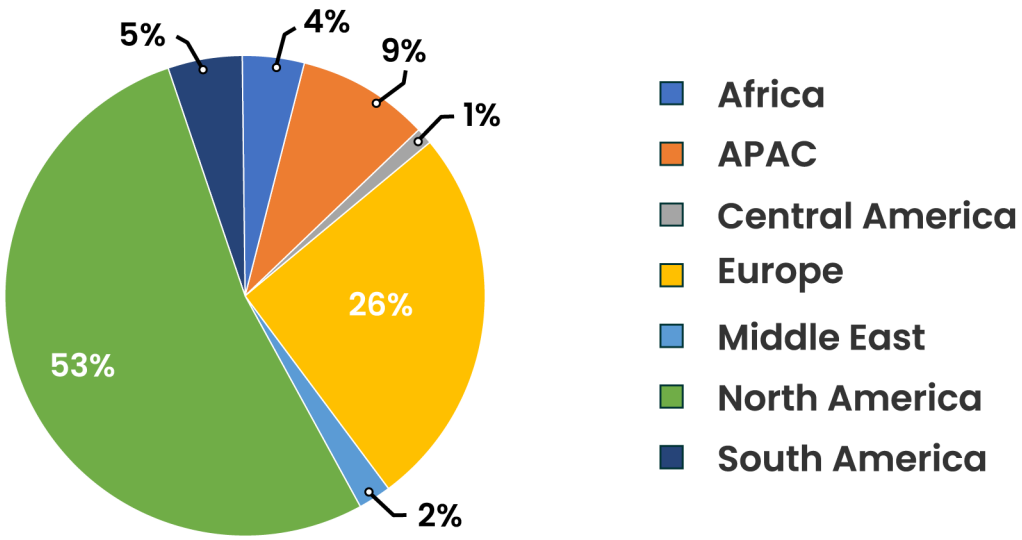
Ransomware Statistics

- Western Digital compromised by AlphVM ransomware.
- Darktrace, an intelligence company compromised by Lockbit ransomware.

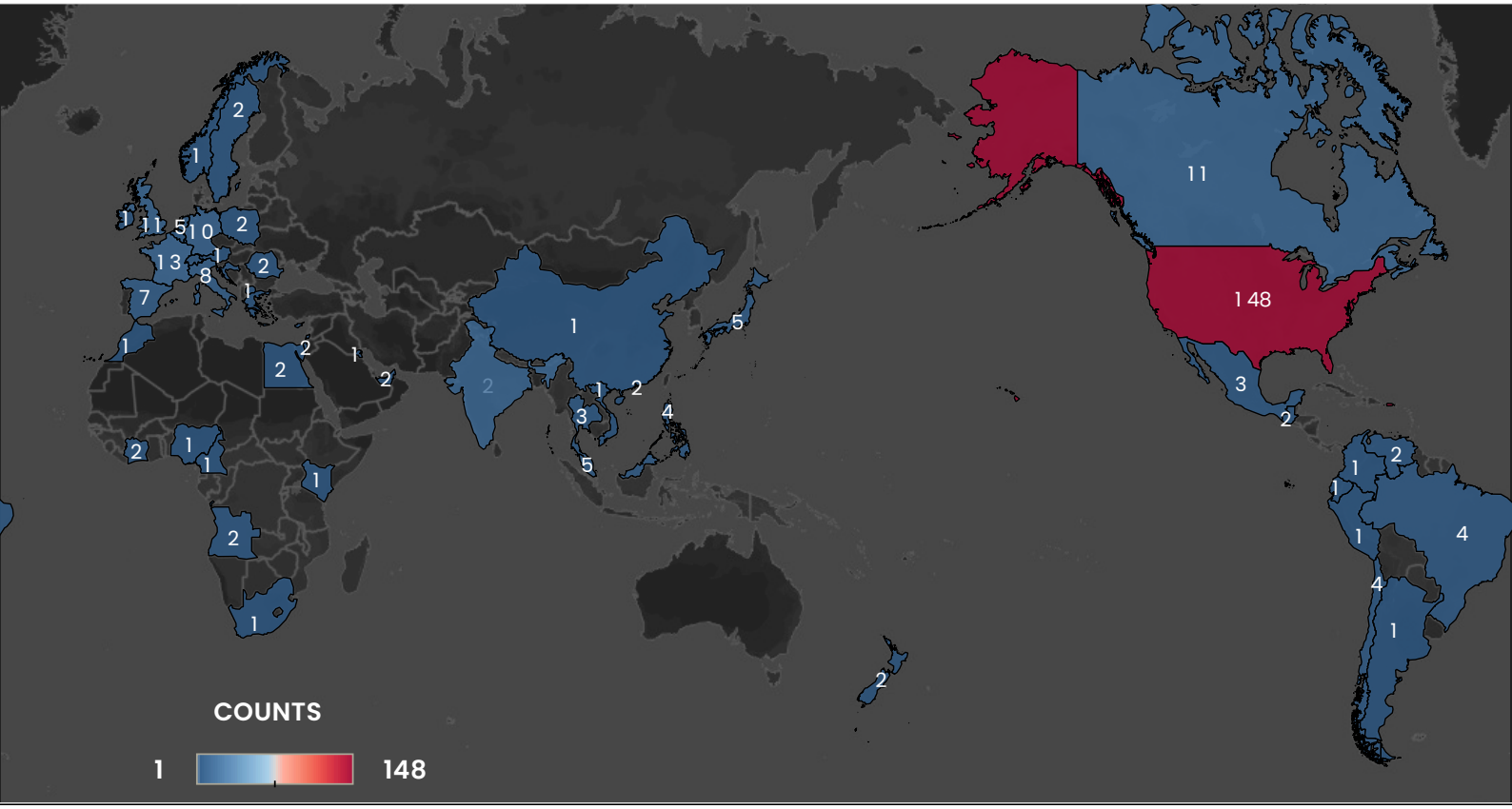




REGION-WISE ATTACK



COUNTRY-WISE ATTACK TREND - 299



02

North Korean Nexus Identified Threat Actors in 3CX Incident

Tags: 3CX, Telecom, IT, USA, Supply Chain Attack

In March 2023, 3CX Systems, a pioneer in business communication solutions and software, announced that it had suffered a massive data breach that had affected its clients. On April 11th, 2023, 3CX's CISO posted on the company's website, an initial update of the Incident Response done by Mandiant.

The threat actor dubbed as UNC4736, a North Korean group has been identified to have compromised a third-party vendor, a trading technologies company, from where 3CX was compromised. The supply chain then took the next turn towards 3CX's customers. The initial compromise was done by targeting a software package of the trading company, dubbed X_TRADER, which deployed VeiledSignal, a multi-stage modular backdoor that performs command injection and communicates with Command & Control Server.

After the execution phase, the actor used publicly available Fast Reverse Proxy Project, to move laterally within the organization and compromised Windows and MacOS build environments. Malwares TAXHAUL, COLDCAT, IKEEXT, and POOLRAT were installed to perform different executions. Threat actor UNC4736 is most likely linked to financially motivated operations.

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

03

Zero-day Vulnerability in Microsoft Windows Targeted by Nokoyawa Ransomware

Tags: Zero day, Windows, Ransomware

On April 11th, 2023, Microsoft updated 1 Zero-day and 97 other vulnerabilities in its systems. The Zero-day vulnerability CVE-2023-28252 actively under attack exists in Windows' core component - Windows Common Log File System (CLFS driver) that allows an adversary with user access privileges to gain system privileges. This happens through exploiting the base log file (.blf), which is a master file created through CLFS driver functions. The adversary attempts to exhaust metadata block of the .blf file which results in out of bound write vulnerability, wherein a specially crafted BLF object allows memory pointers to leak addresses of kernel objects that can be further exploited through other vulnerabilities.

Observed in action by researchers at Kaspersky in Nokoyawa ransomware, the threat group has been targeting retail & wholesale, energy, manufacturing, healthcare, software development, and many other industries.

Other critical vulnerabilities include CVE-2023-28231, CVE-2023-28220, CVE-2023-28219, CVE-2023-28285, CVE-2023-28295, CVE-2023-28287, and CVE-2023-28311.

04

Pakistan-based Threat Actor Targeting Indian Education Sector

Tags: Education, APT 36, Crimson RAT

Active since 2013, Pakistan-based threat actor named APT 36 aka Transparent Tribe, known for its frequent usage of Crimson RAT malware, has been identified to have recently targeted the education sector of India, researchers at Sentinel One suggest. Using the technique T1566.001, that is Spear phishing via attachment, the threat actor has been circulating educational content-like assignments. This is being shared over email and hosted on multiple file-sharing platforms and malicious domains.

The malicious documents contain macro functions or OLE embeddings, resulting in the creation of an archived file under the ProgramData folder in C drive, executing CrimsonRAT payload inside it. This payload masquerades as a Microsoft update, named Executable, which performs multiple actions like connecting to the C2 domain, establishing persistence through adding a registry key under Windows' current version, and exfiltrating relevant data to the C2 servers.

Given the active involvement and support of students and professors of different institutions in sensitive projects of defense and energy sectors in India, it is very important to safeguard against active attacks.

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

05

FIN7 and Conti Ransomware Work on New Backdoor

Tags: Finance, Ransomware, backdoor

Researchers at IBM X-Force have identified a new backdoor being propagated on the internet, that might have been developed in collaboration with the FIN7 threat group and a faction of Conti Ransomware developers. This report comes after researchers identified the Dave loader, a loader developed by the Conti team to be loading a new backdoor named "DOMINO" after effectively using Dave loader to deploy IcedID and Emotet. These have been used as initial access vectors for ransomware attacks like Quantum, Royal, BlackBasta, and Zeon.

Domino backdoor gathers basic information about a system and sends it back to its Command & Control. This information enables the C2 to then identify and send back an AES encrypted payload to the system. Dubbed as Domino Loader, this payload decrypts into a .NET infostealer identified as part of 'Project Nemesis'.

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

06

Taxpayers on the Radar of Threat Actors as the Tax Return Dates Approach

Tags: Finance, Scams, Malware

As the tax month approached in India and the US, various threat actors leveraged the opportunity to perform social engineering attacks. Microsoft observed phishing attacks targeting accounting and tax return propagation firms to deliver REMCOS remote access trojan (RAT) compromising networks, since February 2023.

In this instance, the targets are organizations that deal with tax preparation, financial services, accounting, and professional bookkeeping. The malware masquerades as a tax document shared by the client, which redirects the victim employee to a legitimate file hosting site uploaded as Windows-based .lnk files.The LNK files generate web requests to IP/domains controlled by the attacker to download malicious files. Depending on the system configuration where the file is downloaded, the REMCOS payload is downloaded for further exploitation of device and network.

In another instance of targeting Tax firms, researchers at Sophos shared how phishing attacks with file attachments were seen. The attachments consisted of ZIP files containing shortcut labelled as a PDF file, which is actually a VBScript invoking web requests to a malicious domain. The domain has GuLoader malware that performs further exploitation.

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

07

Qbot Malware Being Spread via Business Letters

Tags: Cloud, Qbot, QuackBot, Pinkslipbot

Researchers at Kaspersky detected Qbot banking trojan being spread through business letters across continents. In April, researchers came across multiple email letters written in different languages like English, German, Italian, and French that were based on real email letters. These email letters contained PDF files as malicious attachments (T1566.001) originating from the fraudulent email addresses of legitimate users from previous conversations.

Active since 2007, Qbot family has made modifications from time to time, evolving and improving its capabilities. With Cloud emergence, the malware targets Microsoft Office 365 or Azure by imitating the alerts to open the attachments. Once clicked, an archive file is downloaded from a remote malicious server, containing a WSF(Windows Script File) obfuscating a JScript. The script executes a PowerShell that downloads a library, which is the Qbot malware.

The malware is capable of extracting passwords and cookies from browsers, stealing letters from mailboxes, monitoring traffic, and providing the attacker, the remote access to the system. Further actions and extractions are dependent on the target value of the victim's system as assessed by attacker.

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

08

Trigona Ransomware Targeting MS-SQL Servers

Tags: Microsoft, Ransomware, SQL

Active since June 2022, the Trigona ransomware family is written in Delphi language which uses double extortion techniques. This means that the ransomware exfiltrates the files and at the same time encrypts them on victims' computers. Researchers at ASEC Labs identified the Trigona ransomware targeting poorly managed MS-SQL servers.

MS-SQL servers with default credentials, simple passwords that can be brute forced, and servers with publicly visible connections have been targeted most frequently in the campaign. According to reports, once logged in, the victim machine is installed with CLR Shell malware, which sets up an interactive environment for the Trigona malware to be installed. Once installed and executed under svcservice[.]exe process, a dropper malware takes the process name sqlservr[.]exe, which then goes on to create and execute the actual Trigona ransomware as svchost.exe in the same path as svcservice.

Using a bat file, the malware is executed followed by updating the registry key for persistence. The ransomware typically utilizes 4112-bit RSA and 256-bit AES encryption techniques for file encryption.

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

09

Lockbit Ransomware Now Targets MacOS Systems

Tags: MacOS, IT, Lockbit, ransomware

After wreaking havoc in different industries by targeting Microsoft Windows systems and Linux systems (since January 2022), Lockbit ransomware developers have now set their eyes on MacOS systems. Threat Researchers who go by the name Malwarehunterteam on Twitter have identified the ransomware and researchers at SentinelOne have shared details of a Lockbit variant that seems to be targeting the Apple MacOS arm64 architecture.

Even though there are no public claims of victims targeted by the variant, the analysis of the samples suggest that Lockbit continues to target and extort organizations. Malware that can be executed by a human operator or a configuration file targets a list of hardcoded extensions some of which don't belong to the MacOS system. An operator can specify which type of files can be encrypted. When executing on an Apple M1 or M2 device, the ransomware checks the hw.model to identify model details, as a part of anti-analysis feature.

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

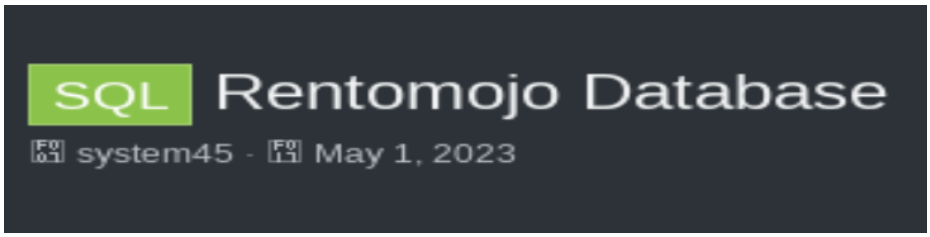
10

Shiny Hunters Compromise Indian Startup RentoMojo

Tags: RentoMojo, IT, Shiny Hunter

An online furniture and motorbike rental startup, RentoMojo, was compromised by the Shiny Hunter group in April. The threat group, in an unusual approach, emailed a few of the company's customers with certain proof that they had compromised RentoMojo was compromised and large amounts of data was exfiltrated. This data included KYC details, bank details and other sensitive documents, the news of which was shared by users on Twitter.

RentoMojo on April 20th, reported that in the data breach over one lakh customer records were compromised. Through an email to its customers, the company shared that Shiny Hunters got access to a misconfigured cloud instance, breaching one of the databases. A user going by the name "system45" posted on a Russian dark web forum on May 1st, two zipped folders, sized 10GB, which on processing and unzipping, result computing to a massive 295GB approximately. No major updates have been received from the RentoMojo team who is aiming to have a better security infrastructure, only post the attack.



Shiny Hunters, who have been active since 2020, has made its name in the black hat community through a series of major compromises and claims, such as, exfiltrating Microsoft source code from their GitHub repository, photo editing application – pixlr, and heavily attacking Indian companies in past few years. Some of the targets include BuyUcoin – a cryptocurrency wallet, Bigbasket – Online Grocery Store, JusPay – Payment Gateway, etc. The unique reconnaissance technique used by the group involves identifying its potential targets through Microsoft Office 365

11

Appendix

Appendix 1A – UNC4736, 3CX attack

Yara Detection Rules

rule M_Hunting_3CXDesktopApp_Key {
meta:
disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
description = "Detects a key found in a malicious 3CXDesktopApp file"
md5 = "74bc2d0b6680faa1a5a76b27e5479cbc"
date = "2023/03/29"
version = "1"
strings:
$key = "3jB(2bsG#@c7" wide ascii
condition:
$key
}

rule M_Hunting_3CXDesktopApp_Export {
meta:
disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
description = "Detects an export used in 3CXDesktopApp malware"
md5 = "7faea2b01796b80d180399040bb69835"
date = "2023/03/31"
version = "1"
strings:
$str1 = "DllGetClassObject" wide ascii
$str2 = "3CXDesktopApp" wide ascii
condition:
all of ($str*)
}

```
rule TAXHAUL
 {
  meta:
  author = “Mandiant”
  created = “04/03/2023”
  modified = “04/03/2023”
  version = “1.0”
  strings:
   $p00_0 = {410f45fe4c8d3d[4]eb??4533f64c8d3d[4]eb??4533f-
64c8d3d[4]eb}
   $p00_1 = {4d3926488b01400f94c6ff90[4]41b9[4]eb??8bde4885c074}
  condition:
   uint16(0) == 0x5A4D and any of them
 }
```

```
rule M_Hunting_MSI_Installer_3CX_1
 {
 meta:
 author = “Mandiant”
 md5 = “0eeb1c0133eb4d571178b2d9d14ce3e9, f3d4144860ca10ba60f7ef4d-
176cc736”
 strings:
 $ss1 = { 20 00 5F 64 33 64 63 6F 6D 70 69 6C 65 72 5F 34 37 2E 64 6C 6C 5F
}
 $ss2 = { 20 00 5F 33 43 58 44 65 73 6B 74 6F 70 41 70 70 2E }
 $ss3 = { 20 00 5F 66 66 6D 70 65 67 2E 64 6C 6C 5F }
 $ss4 = “3CX Ltd1” ascii
 $sc1 = { 1B 66 11 DF 9C 9A 4D 6E CC 8E D5 0C 9B 91 78 73 }
 $sc2 = “202303” ascii
 condition:
 (uint32(0) == 0xE011CFD0) and filesize > 90MB and filesize < 105MB and all
of them
 }
```

```
rule M_Hunting_TAXHAUL_Hash_1
 {
 meta:
 author = "Mandiant"
 disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
 description = "Rule looks for hardcoded value used in string hashing algorithm observed in instances of TAXHAUL."
 md5 = "e424f4e52d21c3da1b08394b42bc0829"
 strings:
 $c_x64 = { 25 A3 87 DE [4-20] 25 A3 87 DE [4-20] 25 A3 87 DE }
 condition:
 filesize < 15MB and uint16(0) == 0x5a4d and uint32(uint32(0x3C)) == 0x00004550 and any of them
 }
```

```
rule M_Hunting_SigFlip_SigLoader_Native
 {
 meta:
 author = "Mandiant"
 disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
 description = "Rule looks for strings present in SigLoader (Native)"
 md5 = "a3ccc48db9eabfed7245ad6e3a5b203f"
 strings:
 $s1 = "[*]: Basic Loader..." ascii wide
 $s2 = "[!]: Missing PE path or Encryption Key..." ascii wide
 $s3 = "[!]: Usage: %s <PE_PATH> <Encryption_Key>" ascii wide
 $s4 = "[*]: Loading/Parsing PE File '%s'" ascii wide
 $s5 = "[!]: Could not read file %s" ascii wide
 $s6 = "[!]: '%s' is not a valid PE file" ascii wide
 $s7 = "[+]: Certificate Table RVA %x" ascii wide
 $s8 = "[+]: Certificate Table Size %d" ascii wide
 $s9 = "[*]: Tag Found 0x%x%x%x%x" ascii wide
 $s10 = "[!]: Could not locate data/shellcode" ascii wide
 $s11 = "[+]: Encrypted/Decrypted Data Size %d" ascii wide
 condition:
 filesize < 15MB and uint16(0) == 0x5a4d and uint32(uint32(0x3C)) == 0x00004550 and 4 of ($s*)
 }
```

```
ule M_Hunting_Raw64_DAVESHELL_Bootstrap
 {
 meta:
 author = "Mandiant"
 disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
 description = "Rule looks for bootstrap shellcode (64 bit) present in DAVESHELL"
 md5 = "8a34adda5b981498234be921f86dfb27"
 strings:
 $b6ba50888f08e4f39b43ef67da27521dcfc61f1e = { E8 00 00 00 00 59 49 89 C8 48 81 C1 ?? ?? ?? ?? BA ?? ?? ?? ?? 49 81 C0 ?? ?? ?? ?? 41 B9 ?? ?? ?? ?? 56 48 89 E6 48 83 E4 F0 48 83 EC 30 C7 44 24 20 ?? ?? ?? ?? E8 ?? 00 00 00 48 89 F4 5E C3 }
 $e32abbe82e1f957fb058c3770375da3bf71a8cab = { E8 00 00 00 00 59 49 89 C8 BA ?? ?? ?? ?? 49 81 C0 ?? ?? ?? ?? 41 B9 ?? ?? ?? ?? 56 48 89 E6 48 83 E4 F0 48 83 EC 30 48 89 4C 24 28 48 81 C1 ?? ?? ?? ?? C7 44 24 20 ?? ?? ?? ?? E8 ?? 00 00 00 48 89 F4 5E C3 }
 condition:
 filesize < 15MB and any of them
 }
```

```
rule M_Hunting_MSI_Installer_3CX_1
 {
 meta:
 author = "Mandiant"
 disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
 description = "This rule looks for hardcoded values within the MSI installer observed in strings and signing certificate"
 md5 = "0eeb1c0133eb4d571178b2d9d14ce3e9"
 strings:
 $ss1 = { 20 00 5F 64 33 64 63 6F 6D 70 69 6C 65 72 5F 34 37 2E 64 6C 6C 5F }
 $ss2 = { 20 00 5F 33 43 58 44 65 73 6B 74 6F 70 41 70 70 2E }
 $ss3 = { 20 00 5F 66 66 6D 70 65 67 2E 64 6C 6C 5F }
 $ss4 = "3CX Ltd1" ascii
 $sc1 = { 1B 66 11 DF 9C 9A 4D 6E CC 8E D5 0C 9B 91 78 73 }
 $sc2 = "202303" ascii
 condition:
 (uint32(0) == 0xE011CFD0) and filesize > 90MB and filesize < 100MB and all of them
 }
```

```
rule M_Hunting_VEILEDSIGNAL_1
 {
 meta:
 author = "Mandiant"
 disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
 md5 = "404b09def6054a281b41d309d809a428, c6441c961dcad0fe-127514a918eaabd4"
 strings:
 $rh1 = { 68 5D 7A D2 2C 3C 14 81 2C 3C 14 81 2C 3C 14 81 77 54 10 80 26 3C 14 81 77 54 17 80 29 3C 14 81 77 54 11 80 AB 3C 14 81 D4 4C 11 80 33 3C 14 81 D4 4C 10 80 22 3C 14 81 D4 4C 17 80 25 3C 14 81 77 54 15 80 27 3C 14 81 2C 3C 15 81 4B 3C 14 81 94 4D 1D 80 28 3C 14 81 94 4D 14 80 2D 3C 14 81 94 4D 16 80 2D 3C 14 81 }
 $rh2 = { 00 E5 A0 2B 44 84 CE 78 44 84 CE 78 44 84 CE 78 1F EC CA 79 49 84 CE 78 1F EC CD 79 41 84 CE 78 1F EC CB 79 C8 84 CE 78 BC F4 CA 79 4A 84 CE 78 BC F4 CD 79 4D 84 CE 78 BC F4 CB 79 65 84 CE 78 1F EC CF 79 43 84 CE 78 44 84 CF 78 22 84 CE 78 FC F5 C7 79 42 84 CE 78 FC F5 CE 79 45 84 CE 78 FC F5 CC 79 45 84 CE 78}
 $rh3 = { DA D2 21 22 9E B3 4F 71 9E B3 4F 71 9E B3 4F 71 C5 DB 4C 70 94 B3 4F 71 C5 DB 4A 70 15 B3 4F 71 C5 DB 4B 70 8C B3 4F 71 66 C3 4B 70 8C B3 4F 71 66 C3 4C 70 8F B3 4F 71 C5 DB 49 70 9F B3 4F 71 66 C3 4A 70 B0 B3 4F 71 C5 DB 4E 70 97 B3 4F 71 9E B3 4E 71 F9 B3 4F 71 26 C2 46 70 9F B3 4F 71 26 C2 B0 71 9F B3 4F 71 9E B3 D8 71 9F B3 4F 71 26 C2 4D 70 9F B3 4F 71 }
 $rh4 = { CB 8A 35 66 8F EB 5B 35 8F EB 5B 35 8F EB 5B 35 D4 83 5F 34 85 EB 5B 35 D4 83 58 34 8A EB 5B 35 D4 83 5E 34 09 EB 5B 35 77 9B 5E 34 92 EB 5B 35 77 9B 5F 34 81 EB 5B 35 77 9B 58 34 86 EB 5B 35 D4 83 5A 34 8C EB 5B 35 8F EB 5A 35 D3 EB 5B 35 37 9A 52 34 8C EB 5B 35 37 9A 58 34 8E EB 5B 35 37 9A 5B 34 8E EB 5B 35 37 9A 59 34 8E EB 5B 35 }
 condition:
 uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and 1 of ($rh*)
 }
```

```
rule M_Hunting_VEILEDSIGNAL_2
 {
 meta:
 author = “Mandiant”
 disclaimer = “This rule is meant for hunting and is not tested to run in a production environment”
 md5 = “404b09def6054a281b41d309d809a428”
 strings:
 $sb1 = { C1 E0 05 4D 8? [2] 33 D0 45 69 C0 7D 50 BF 12 8B C2 41 FF C2 C1 E8 07 33 D0 8B C2 C1 E0 16 41 81 C0 87 D6 12 00 }
 $si1 = “CryptBinaryToStringA” fullword
 $si2 = “BCryptGenerateSymmetricKey” fullword
 $si3 = “CreateThread” fullword
 $ss1 = “ChainingModeGCM” wide
 $ss2 = “__tutma” fullword
 condition:
 (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x020B) and all of them
 }
```

```
rule M_Hunting_VEILEDSIGNAL_3
 {
 meta:
 author = “Mandiant”
 disclaimer = “This rule is meant for hunting and is not tested to run in a production environment”
 md5 = “c6441c961dcad0fe127514a918eaabd4”
 strings:
 $ss1 = { 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6A 73 6F 6E 2C 20 74 65 78 74 2F 6A 61 76 61 73 63 72 69 70 74 2C 20 2A 2F 2A 3B 20 71 3D 30 2E 30 31 00 00 61 63 63 65 70 74 00 00 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 39 00 00 61 63 63 65 70 74 2D 6C 61 6E 67 75 61 67 65 00 63 6F 6F 6B 69 65 00 00 }
 $si1 = “HttpSendRequestW” fullword
 $si2 = “CreateNamedPipeW” fullword
 $si3 = “CreateThread” fullword
 $se1 = “DllGetClassObject” fullword
 condition:
 (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x020B) and all of them
 }
```

```
rule M_Hunting_VEILEDSIGNAL_4
 {
 meta:
 author = "Mandiant"
 disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
 md5 = "404b09def6054a281b41d309d809a428, c6441c961dcad0fe-127514a918eaabd4"
 strings:
 $sb1 = { FF 15 FC 76 01 00 8B F0 85 C0 74 ?? 8D 50 01 [6-16] FF 15 [4] 48 8B D8 48 85 C0 74 ?? 89 ?? 24 28 44 8B CD 4C 8B C? 48 89 44 24 20 }
 $sb2 = { 33 D2 33 C9 FF 15 [4] 4C 8B CB 4C 89 74 24 28 4C 8D 05 [2] FF FF 44 89 74 24 20 33 D2 33 C9 FF 15 }
 $si1 = "CreateThread" fullword
 $si2 = "MultiByteToWideChar" fullword
 $si3 = "LocalAlloc" fullword
 $se1 = "DllGetClassObject" fullword
 condition:
 (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x020B) and all of them
 }
```

```
rule M_Hunting_VEILEDSIGNAL_5
 {
 meta:
 author = "Mandiant"
 disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
 md5 = "6727284586ecf528240be21bb6e97f88"
 strings:
 $sb1 = { 48 8D 15 [4] 48 8D 4C 24 4C E8 [4] 85 C0 74 ?? 48 8D 15 [4] 48 8D 4C 24 4C E8 [4] 85 C0 74 ?? 48 8D 15 [4] 48 8D 4C 24 4C E8 [4] 85 C0 74 ?? 48 8D [3] 48 8B CB FF 15 [4] EB }
 $ss1 = "chrome.exe" wide fullword
 $ss2 = "firefox.exe" wide fullword
 $ss3 = "msedge.exe" wide fullword
 $ss4 = "\\\\.\\pipe\\*" ascii fullword
 $ss5 = "FindFirstFileA" ascii fullword
 $ss6 = "Process32FirstW" ascii fullword
 $ss7 = "RtlAdjustPrivilege" ascii fullword
 $ss8 = "GetCurrentProcess" ascii fullword
 $ss9 = "NtWaitForSingleObject" ascii fullword
 condition:
 (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x020B) and all of them
 }
```

```
rule M_Hunting_VEILEDSIGNAL_6
 {
 meta:
 author = "Mandiant"
 disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
 md5 = "00a43d64f9b5187a1e1f922b99b09b77"
 strings:
 $ss1 = "C:\\Programdata\\" wide
 $ss2 = "devobj.dll" wide fullword
 $ss3 = "msvcr100.dll" wide fullword
 $ss4 = "TpmVscMgrSvr.exe" wide fullword
 $ss5 = "\\Microsoft\\Windows\\TPM" wide fullword
 $ss6 = "CreateFileW" ascii fullword
 condition:
 (uint16(0) == 0x5A4D) and (uint32(uint32(0x3C)) == 0x00004550) and (uint16(uint32(0x3C)+0x18) == 0x010B) and all of them
 }
```

```
rule M_Hunting_POOLRAT
 {
 meta:
 author = "Mandiant"
 disclaimer = "This rule is meant for hunting and is not tested to run in a production environment"
 description = "Detects strings found in POOLRAT. "
 md5 = "451c23709ecd5a8461ad060f6346930c"
 strings:
 $hex1 = { 6e 61 6d 65 3d 22 75 69 64 22 25 73 25 73 25 75 25 73 }
 $hex_uni1 = { 6e 00 61 00 6d 00 65 00 3d 00 22 00 75 00 69 00 64 00 22 00 25 00 73 00 25 00 73 00 25 00 75 00 25 00 73 }
 $hex2 = { 6e 61 6d 65 3d 22 73 65 73 73 69 6f 6e 22 25 73 25 73 25 75 25 73 }
 $hex_uni2 = { 6e 00 61 00 6d 00 65 00 3d 00 22 00 73 00 65 00 73 00 73 00 69 00 6f 00 6e 00 22 00 25 00 73 00 25 00 73 00 25 00 75 00 25 00 73 }
 $hex3 = { 6e 61 6d 65 3d 22 61 63 74 69 6f 6e 22 25 73 25 73 25 73 25 73 }
 $hex_uni3 = { 6e 00 61 00 6d 00 65 00 3d 00 22 00 61 00 63 00 74 00 69 00 6f 00 6e 00 22 00 25 00 73 00 25 00 73 00 25 00 73 00 25 00 73 }
 $hex4 = { 6e 61 6d 65 3d 22 74 6f 6b 65 6e 22 25 73 25 73 25 75 25 73 }
 $hex_uni4 = { 6e 00 61 00 6d 00 65 00 3d 00 22 00 74 00 6f 00 6b 00 65 00 6e 00 22 00 25 00 73 00 25 00 73 00 25 00 75 00 25 00 73 }
 $str1 = "--N9dLfqxHNUUw8qaUPqggVTpX-" wide ascii nocase
 condition:
 any of ($hex*) or any of ($hex_uni*) or $str1
 }
```

```
rule M_Hunting_FASTREVERSEPROXY
 {
      meta:
      author = "Mandiant"
      disclaimer = "This rule is meant for hunting and is not tested to run in a
production environment"
      md5 = "19dbffec4e359a198daf4ffca1ab9165"
      strings:
      $ss1 = "Go build ID:" fullword
      $ss2 = "Go buildinf:" fullword
      $ss3 = "net/http/httputil.(*ReverseProxy)." ascii
      $ss4 = "github.com/fatedier/frp/client" ascii
      $ss5 = "\"server_port\"" ascii
      $ss6 = "github.com/armon/go-socks5.proxy" ascii
      condition:
      uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and all
of them
 }
```

Snort Rules
alert tcp any any -> any any (msg:"Possible malicious 3CXDesktopApp Identified"; content:"raw.githubusercontent.com/IconStorages/images/main/"; threshold:type limit, track by_src, count 1, seconds 3600; sid: 99999999;)
alert tcp any any -> any any (msg:"Possible malicious 3CXDesktopApp Identified"; content:"3cx_auth_id=%s\;3cx_auth_token_content=%s\;__tutma=true"; threshold:type limit, track by_src, count 1, seconds 3600; sid: 99999999;)
alert tcp any any -> any any (msg:"Possible malicious 3CXDesktopApp Identified"; content:"__tutma"; threshold:type limit, track by_src, count 1, seconds 3600; sid: 99999999;)
alert tcp any any -> any any (msg:"Possible malicious 3CXDesktopApp Identified"; content:"__tutmc"; threshold:type limit, track by_src, count 1, seconds 3600; sid: 99999999;)

Appendix 1B – APT36

SHA1	Description
738d31ceca78ffd053403d3b2b-c15847682899a0	Malicious document
9ed39c6a3faab057e6c962f-0b2aaab07728c5555	Malicious document
af6608755e2708335dc80961a9e-634f870aecf3c	Malicious document
e000596ad65b2427d7af3313e-5748c2e7f37fba7	Malicious document
fd46411b315beb36926877e4b021721f-cd111d7a	Malicious document
516db7998e3bf-46858352697c1f103ef456f2e8e	Crimson RAT
842f55579db786e46b-20f7a7053861170e1c0c5e	Crimson RAT
87e0ea08713a746d53bef7fb04632b-fcd6717fa9	Crimson RAT
911226d78918b303df5110704a8c8bb-599bcd403	Crimson RAT
973cb3afc7eb47801ff5d-2487d2734ada6b4056f	Crimson RAT

Domain	Description
richa-sharma.ddns[.]net	C2 server
cloud-drive[.]store	Malware hosting location
drive-phone[.]online	Malware hosting location
s1.fileditch[.]ch	Malware hosting location

Appendix 1C – Domino Backdoor

Domain	Indicator Type	Context
de9b3c01991e357a349083f0db6af3e-782f15e981e2bf0a16ba618252585923a	SHA256 Hash	ave Loader / Domino Backdoor
b14ab379ff43c7382c1aa881b2be39275c-1594954746ef58f6a9a3535e8dc1a8	SHA256 Hash	Dave Loader / Domino Backdoor
dbdfc3ca5afa186c1a9a9c03129773f7b-c17fb7988fe0ca40fc3c5bedb201978	SHA256 Hash	Dave Loader / Domino Backdoor
ce99b4c0d75811ce70610d39b-1007f99560e6dea887a451e08916a4f-8cf33678	SHA256 Hash	Dave Loader / Domino Backdoor
f1817665ea2831f775e23cbdwa27cbeb-06d03e6c39bbfad920b50f40712dd37cb	SHA256 Hash	NewWorldOrder Loader / Carbanak Backdoor
51e0512a54640be8e3477363c8d-72d893c6edd20399bddf71e95e-ec3ddfdb42e	SHA256 Hash	NewWorldOrder Loader / Carbanak Backdoor
f4ebd59fb578a0184abf6870fc-652210d63e078a35dace0a48c5f-273e417c13d	SHA256 Hash	NewWorldOrder Loader / Carbanak Backdoor
92651f9418625e5281b84cccb817e94e-6294b36c949b00fcd4046770b87f10e4	SHA256 Hash	NewWorldOrder Loader / Carbanak Backdoor
e5af0b9f4650dc-0193c9884507e6202b04bb87ac5ed-261be3f4ecfa3b6911af8	SHA256 Hash	Domino Backdoor
hxxp://170.130.55[.]250/x64.exe	URL	Staging URL for Domino Backdoor
hxxps://upperdunk[.]com/mr64.exe	URL	Staging URL for Domino Backdoor
88.119.175[.]124	IP Address	Domino Backdoor C2
94.158.247[.]72	IP Address	Domino Backdoor C2
178.23.190[.]73	IP Address	Carbanak C2
es-megadom[.]com	Domain	Project Nemesis C2
185.225.17[.]202	IP Address	Domino Backdoor C2
5.182.37[.]118	IP Address	Domino Backdoor C2
45.67.34[.]236	IP Address	Project Nemesis C2

Appendix 1D – Tax themed attacks

Domains
uymm[.]org
mhttps[:]//uymm[.]org/roman.msi

SHA-256 hashes
23597910ec60cf8b97144447c5cddd2e657d09e2f2008d53a3834b-6058f36a41
95a2d34db66ce4507d05ac33bea3bdc054860d9d97e91bdc2ce7ce-689ae06e9f
ac55905e6f5a2ab166f9a2ea7d1f4f68f5660f39b5c28b7746df1e9db6dd4430

Appendix 1E – Qbot

MD5
253E43124F66F4FAF23F9671BBBA3D98
39FD8E69EB4CA6DA43B3BE015C2D8B7D
299FC65A2EECF5B9EF06F167575CC9E2
A6120562EB673552A61F7EEB577C05F8
1FBFE5C1CD26C536FC87C46B46DB754D
FD57B3C5D73A4ECD03DF67BA2E48F661
28C25753F1ECD5C47D316394C7FCEDE2

Malicious links
cica.com[.]co/stai/stai.php
abhishekmeena[.]in/ducs/ducs.php
rosewoodlaminates[.]com/hea/yWY9SJ4VOH
agtendelperu[.]com/FPu0Fa/EpN5Xvh
capitalperurrhh[.]com/vQ1iQg/u6oL8xlJ
centerkick[.]com/lC5EQ8/2v6u6vKQwk8
chimpcity[.]com/h7e/p5FuepRZjx
graficalevi.com[.]br/0p6P/R94icuyQ
kmphi[.]com/FWovmB/8oZ0BOV5HqEX
propertynear.co[.]uk/QyYWyp/XRgRWEdFv
theshirtsummit[.]com/MwBGSm/lGP5mGh

Appendix 1F – Trigona ransomware

MD5
1cece45e368656d322b68467ad1b8c02
530967fb3b7d9427552e4ac181a37b9a
1e71a0bb69803a2ca902397e08269302
46b639d59fea86c21e5c4b05b3e29617
5db23a2c723cbceabec8d5e545302dc4

Appendix 1G – Lockbit for MacOS

File name	SHA1
locker_Apple_M1_64	2d15286d25f0e0938823dcd742b-c928e78199b3d
locker_Apple_M1_64	64f56b25a34e9532a1175d469715d2f-61c56f7f
!!!-Restore-My-Files-!!!	ef958f3cf201f9323ceae9663d-86464021f8e10d

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.