GOHSEP Cybersecurity

CYBER THREAT INTEL BRIEF

7 NOV 24

Agenda

- Section 1 : Cyber Threat Intelligence Overview
- Section 2 : Cyber Threat Intelligence Brief
- Section 3 : OT/ICS Threat Intelligence Brief

Section 1

Cyber Threat Intelligence Overview

What is Cyber Threat Intelligence (CTI)?

- CTI provides an organization of what current attacks they could face and how to defend their environment.
- CTI involves gathering data and uncovering trends and patterns to develop a strategy to defend against attacks.
- CTI provides insights needed to understand who may attack and how to properly defend an environment.

Categories of CTI

- Strategic – Focused on High Level Trends, motivations and impacts. Used to forecast decisions on security policies and Investments.
- Tactical – Focused on Tactics, techniques and procedures (TTPs) used by threat actors. Used by Cyber Security teams to understand threat landscapes and prepare their defenses.
- Technical – Detailed info about Indicators of Compromise (IOCs) and the associated threats. Used to detect and block malicious activities.

Sources of CTI

- Open-Source Intel (OSINT) – Publicly available from websites, social media and other platforms.
- Human Intel (HUMINT) – Information from human sources such as insider tips and Interviews.
- Technical Intel (TECHINT) – Data from network analyst that identified malware and observing attack patterns.
- Dark Web – Insights from Dark Web forms, sites and marketplaces where actors share information.
- Premium Intel Feeds - Paid for feeds provided by a vendor that updates IOCs and Emerging Threats.

Free Cyber Threat Intelligence

- CISA Cyber Threat Information Sharing
- CISA Alerts
- InfraGard
- OTX AlienVault
- CISCO Talos
- Security News Articles
- Threat Reports from Popular Vendors such as Palo Alto Unit 42, CrowdStrike, and Mandiant.

Paid Threat Intelligence

- CrowdStrike
- Google Threat Intel
- Recorded Future
- Palo Alto Unit 42
- Dataminer
- Greynoise

Ways to receive Threat Intelligence

- Emails
- Visiting Websites and researching
- Blogs and Forms
- STIX/TAXII (Structured Threat Information eXpression & Trusted Automated eXchange of Intelligence Information)
- Really Simple Syndication (RSS) Feeds
- Threat Intel Platforms (TIPs)

Threat Intelligence Tools

- Threat Intel Platforms
- Virustotal
- Cyber Gordan
- Shodan
- WHOIS
- CENSYS
- NIST National Vulnerability Database

Types of Cyber Threats

- Malware - Malicious software designed to damage or disrupt a system.
- Phishing – Fraudulent message to trick someone into revealing personal information or downloading malware onto their device.
- Ransomware – Malware that encrypts files on a system that demands money for decryption.
- Man In the Middle – Interception and altering of a signal between to systems without their knowledge.

Indicators of Compromise (IOCs)

- Signatures - Known Code that has been associated with Malware
- IP Address/Domain Name – Address of Known Malicious Sites
- File Hashes – Identifies malicious files
- Changes to System Files – Registry or System Dlls that indicate malware presence
- Network Traffic – Unusual Data flow that suggest Exfiltration or movement.

How to Build a Threat Intel Report

- 1-Research and Gather Information
  - Collect data from various sources like OSINT, logs, threat feeds and have an understanding of the landscape.
- 2-Organize and structure the content and start forming a report.
  - Include things such as Executive Summary, Background, Threat Description, IOCs, Impact analysis, Mitigation and recommendations. Make sure to Cite sources to add credibility to report.
- 3-Build and Identify Attacks using MITRE ATT&CK Framework.
- 4-Review and Finalize Report.

Adversaries Naming Conventions

Microsoft

- China – Typhoon
- Iran – Sandstorm
- Lebanon – Rain
- North Korea - Sleet
- Russia – Blizzard
- South Korea – Hail
- Turkey – Dust
- Vietnam – Cyclone

Source: https://infosecwriteups.com/threat-actors-naming-conventions-433da9c5b097

Adversaries Naming Conventions

CrowdStrike

- China – Panda
- Iran – Kitten
- North Korea – Chollima
- India – Tiger
- Syria - Hawk

- Russia – Bear
- South Korea – Crane
- Turkey – Wolf
- Vietnam – Buffalo
- Pakistan – Lopard

Source:https://infosecwriteups.com/threat-actors-naming-conventions-433da9c5b097

Adversaries Naming Conventions

Unit 42 : Palo Alto

- China – Taurus
- Iran – Serpens
- North Korea – Pisces
- India – Gemini
- Russia – Ursa
- Pakistan – Draco
- Belarus – Lynx

Source:https://infosecwriteups.com/threat-actors-naming-conventions-433da9c5b097

Section 2

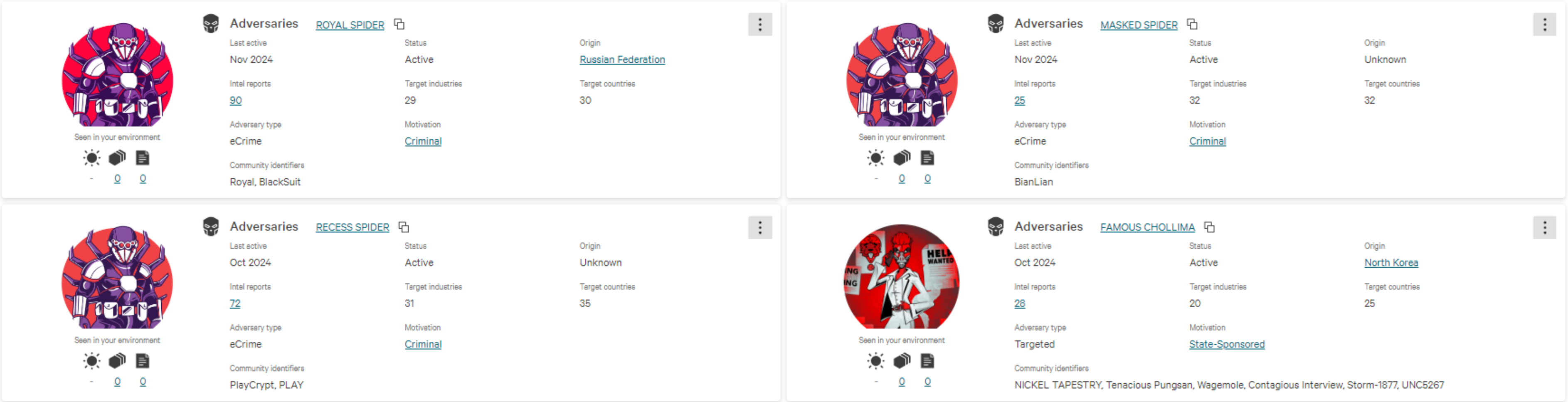
Threat Intelligence Briefing

Top Nation State Cyber Actors

- Chinese Government – Officially known as the People's Republic of China
  - Engages in malicious cyber activities to pursue its national interests including infiltrating critical infrastructure networks.
- Russian Government - Officially known as the Russian Federation
  - Engages in malicious cyber activities to enable broad-scope cyber espionage, to suppress certain social and political activity, to steal intellectual property, and to harm regional and international adversaries.
- North Korean Government - Officially known as the Democratic People's Republic of Korea (DPRK)
  - Employs malicious cyber activity to collect intelligence, conduct attacks, and generate revenue.
- Iranian Government - Officially known as the Islamic Republic of Iran
  - Increased sophisticated cyber capabilities to suppress certain social and political activity, and to harm regional and international adversaries

Source: Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA

Top 4 Threat Actors Targeting Academic Entities



Adversaries ROYAL SPIDER

Last active: Nov 2024
Status: Active
Origin: Russian Federation
Intel reports: 90
Target industries: 29
Target countries: 30
Adversary type: eCrime
Motivation: Criminal
Community identifiers: Royal, BlackSuit
Seen in your environment: - 0 0

Adversaries MASKED SPIDER

Last active: Nov 2024
Status: Active
Origin: Unknown
Intel reports: 25
Target industries: 32
Target countries: 32
Adversary type: eCrime
Motivation: Criminal
Community identifiers: BianLian
Seen in your environment: - 0 0

Adversaries RECESS SPIDER

Last active: Oct 2024
Status: Active
Origin: Unknown
Intel reports: 72
Target industries: 31
Target countries: 35
Adversary type: eCrime
Motivation: Criminal
Community identifiers: PlayCrypt, PLAY
Seen in your environment: - 0 0

Adversaries FAMOUS CHOLLIMA

Last active: Oct 2024
Status: Active
Origin: North Korea
Intel reports: 28
Target industries: 20
Target countries: 25
Adversary type: Targeted
Motivation: State-Sponsored
Community identifiers: NICKEL TAPESTRY, Tenacious Pungsan, Wagemole, Contagious Interview, Storm-1877, UNC5267
Seen in your environment: - 0 0

Source: Adversaries | Counter Adversary Operations |Falcon(crowdstrike.com)

ROYAL SPIDER

- **First Seen :** September 2022
- **Origin :** Russian Federation
- **Description :** ROYAL SPIDER is the adversary behind the development of the Royal and BlackSuit ransomware and the operation of the Ransomware-as-a-Service (RaaS) programs under the same name. In September 2022, ROYAL SPIDER introduced the Royal RaaS as successor to the short-lived Zeon ransomware, which was likely privately operated. Both Royal and BlackSuit ransomware have versions for Windows and Linux/ESXi.   Intelligence has observed ROYAL SPIDER affiliates use commodity malware as well as legitimate tools. Affiliates exfiltrate the sensitive victim data and deploy ransomware to encrypt data on victim systems. The Tactics, Techniques, and Procedures (TTPs) observed in intrusions attributed to ROYAL SPIDER affiliates overlap with those of actors who previously used WIZARD SPIDER's Conti and Ryuk ransomware families.
- **Identifiers :** Royal, Blacksuit

Source: Adversaries | Counter Adversary Operations |Falcon(crowdstrike.com)

RECESS SPIDER

- **First Seen : June 2022**
- **Origin : Unknown**
- **Description :** RECESS SPIDER—publicly tracked as PLAY or PlayCrypt—is a Big Game Hunting (BGH) adversary. RECESS SPIDER develops and privately operates PLAY ransomware. In addition to PLAY ransomware, the adversary uses the custom discovery and defense evasion tool GRB_NET. RECESS SPIDER has continuously evolved their Tactics, Techniques, and Procedures (TTPs) since their discovery. While the adversary initially exploited vulnerable WordPress instances to achieve initial access, the RECESS SPIDER eventually moved on to a new exploit method: Outlook Web Application Server-Side Request Forgery (OWASSRF). Alongside the adversary's operational security measures, this suggests RECESS SPIDER is likely a sophisticated Big Game Hunting (BGH) adversary. The adversary publishes victim data on the dedicated leak site (DLS) PLAY NEWS.
- **Identifiers :** PlayCrypt, PLAY

Source: Adversaries | Counter Adversary Operations |Falcon(crowdstrike.com)

Top Threats Impacting Louisiana

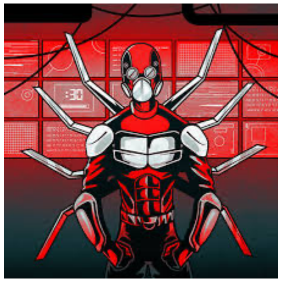
- Punk Spider – Akira Ransomware
- Holiday Spider – HIVE Ransomware
- Masked Spider – Bian Lian Ransomware
- Rancoz Ransomware Group

PUNK SPIDER

- **First Seen :** April 2023
- **Origin :** Unknown
- **Description :** PUNK SPIDER is the Big Game Hunting (BGH) adversary (first identified in April 2023) responsible for developing and maintaining Akira ransomware and its associated Akira dedicated leak site (DLS). PUNK SPIDER relies on sensitive data exfiltration and encryption to extort ransom payments from victims.
- **Identifiers :** Akira, REDBIKE

Source: Adversaries | Counter Adversary Operations | Falcon (crowdstrike.com)

HOLIDAY SPIDER



- **First Seen :** April 2022
- **Origin :** Unknown
- **Description :** HOLIDAY SPIDER, self-named as Daixin Team, is an eCrime and Big Game Hunting (BGH) adversary that has conducted ransomware operations since at least April 2022, initially operating as an affiliate of HIVE SPIDER's Hive Ransomware-as-a-Service (RaaS). HOLIDAY SPIDER relies on encryption and data exfiltration to extort payments from victims. HOLIDAY SPIDER uses Babuk Locker binaries compiled from previously leaked source code as well as legitimate tools to perform their criminal activities, which, to date, has involved the adversary favoring the targeting of healthcare entities.
- **Identifiers :** Daixin Team

Source: Adversaries | Counter Adversary Operations | Falcon (crowdstrike.com)

MASKED SPIDER

- **First Seen : April 2022**
- **Origin: Unknown**
- **Description :** MASKED SPIDER is an opportunistic Big Game Hunting (BGH) eCrime adversary. MASKED SPIDER is responsible for the development and likely private operation of BianLian ransomware. The ransomware encrypts files with AES-256 using hard-coded key information and targets Microsoft Windows and VMware ESXi platforms. The adversary heavily relies on a modified version of the Rsocks reverse-proxy tool and a CLFS LPE tool they likely purchased or acquired from a third party.
- **Identifiers:** BianLian

Source: Adversaries | Counter Adversary Operations | Falcon (crowdstrike.com)

Rancoz Ransomware Group

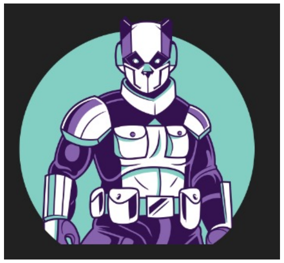
- **First Seen :** November 2022
- **Origin :** Unknown
- **Description :** An observed Threat actor that has compiled and rebranded leaked source code to create a new variant of Ransomware. This approach has allowed the RANCOZ Group to tailor the attacks by Industry and environment.
- **Identifiers :** REC_RANS.EXE

Source: Cyble - Dissecting Rancoz Ransomware

Section 3

OT/ICS Threat Intelligence Brief

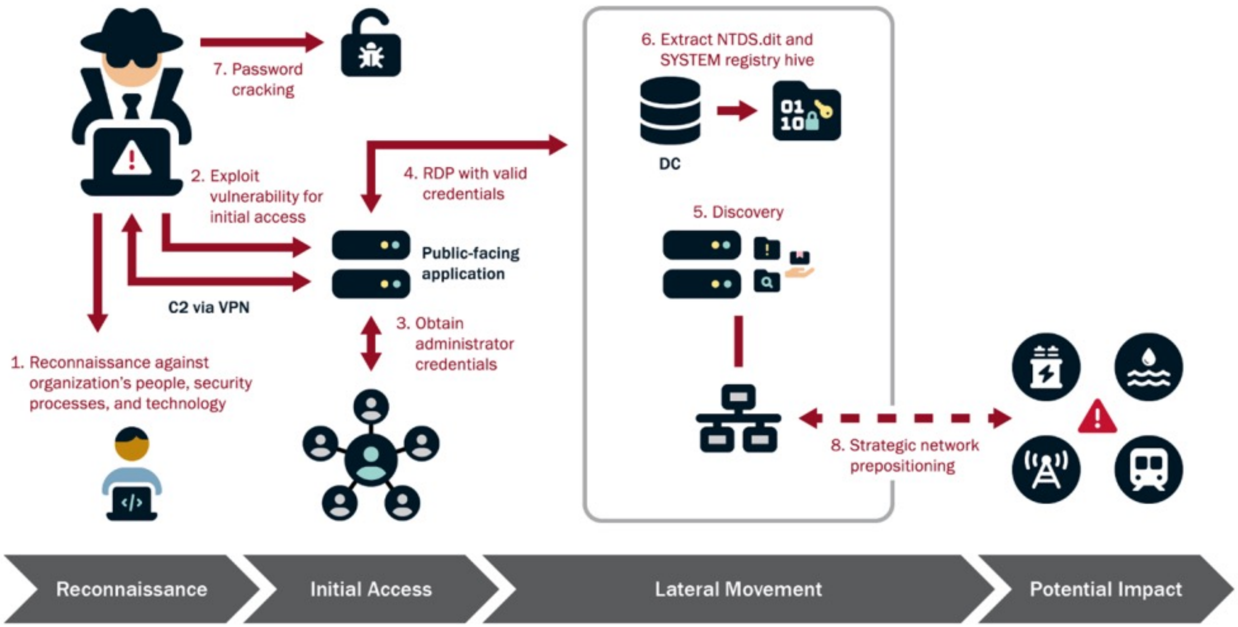
Attacks on Critical Infrastructure : Volt Typhoon/ Vanguard Panda



- **First Seen :** August 2024
- **Origin :** China
- **Description :** VANGUARD PANDA is a China-nexus targeted intrusion adversary that relies heavily on living-off-the-land (LOTL) techniques and uses web shells in addition to well-known tools such as Impacket and Fast Reverse Proxy (FRP). VANGUARD PANDA appears to focus on data such as credentials, likely indicating the group may be tasked with initial access and persistence. The adversary's infrastructure Tactics, Techniques, and Procedures (TTPs) include the use of IP addresses hosting likely compromised small office/home office (SOHO) network equipment—such as routers, firewalls, and virtual private network (VPN) hardware.
- **Identifiers :** Volt Typhoon, BRONZE SILHOUETTE

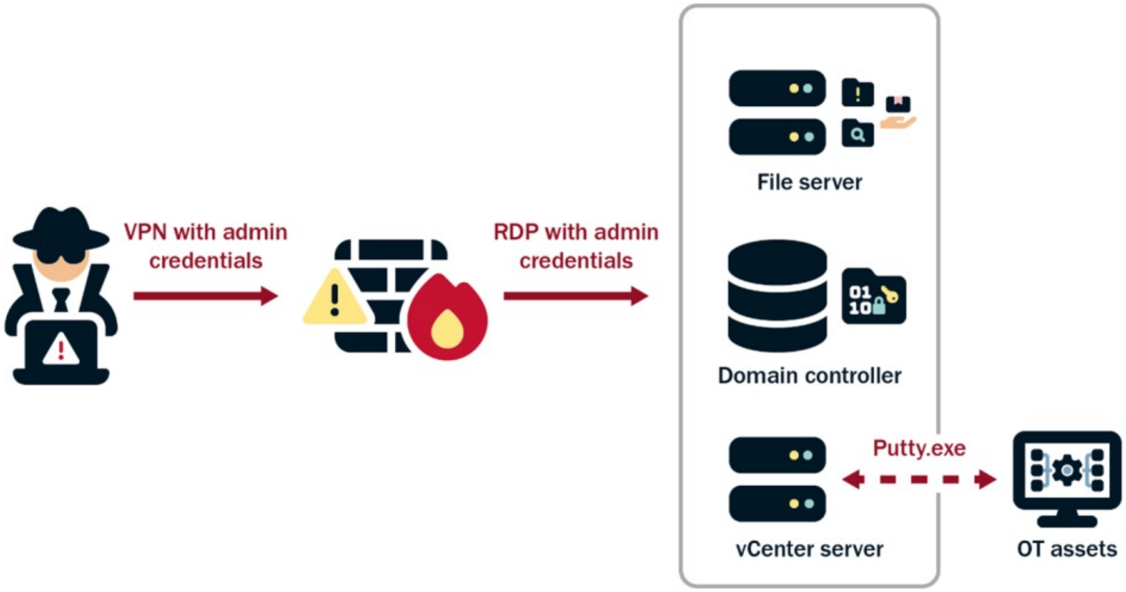
Source: Adversaries | Counter Adversary Operations | Falcon (crowdstrike.com)

So How does this Happen? Phase 1


7. Password cracking
2. Exploit vulnerability for initial access
4. RDP with valid credentials
Public-facing application
C2 via VPN
3. Obtain administrator credentials
1. Reconnaissance against organization's people, security processes, and technology
6. Extract NTDS.dit and SYSTEM registry hive
01 10
DC
5. Discovery
8. Strategic network prepositioning
Reconnaissance
Initial Access
Lateral Movement
Potential Impact

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Phase 2



VPN with admin credentials

RDP with admin credentials

File server

Domain controller

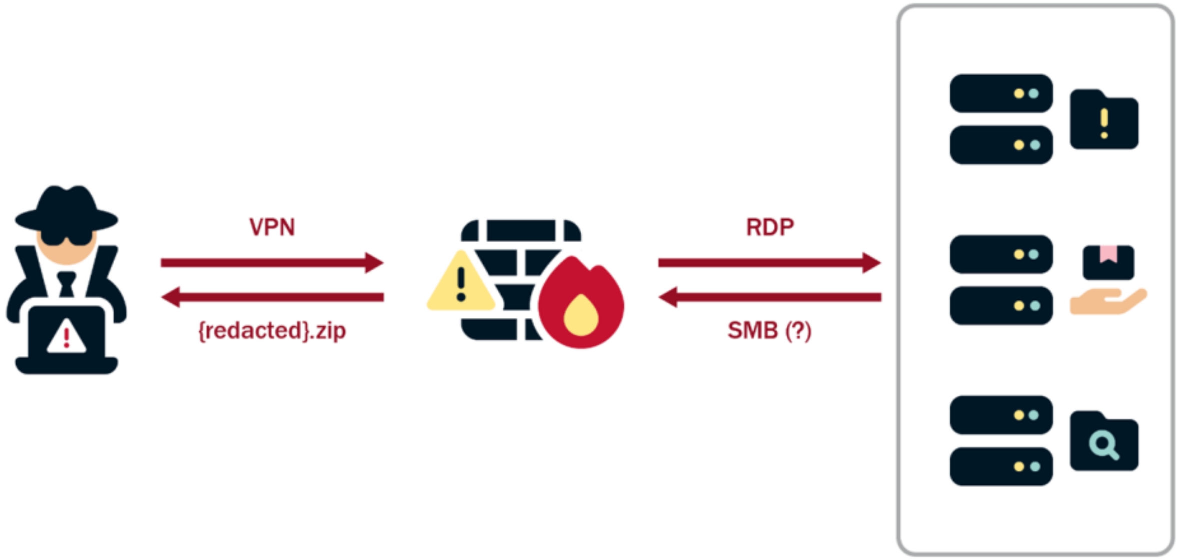
vCenter server

Putty.exe

OT assets

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Phase 3



https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Closing Remarks

CTAC.INTEL@ESF17.la.gov

Keep an eye on getagameplan.org/make-a-plan/cybersecurity-plan/ for cybersecurity tips.