# Cyber Threat Brief

CPT Sean McQuade (Regional Cyber Center – Pacific)

The Overall Classification for this Brief is UNCLASSIFIED

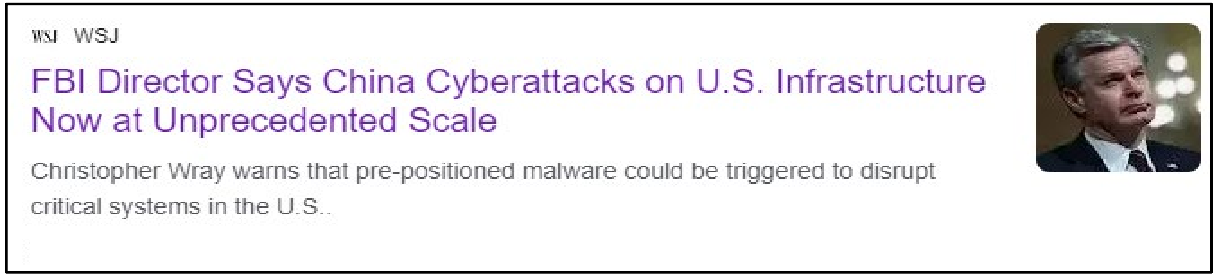
# Disclaimer

The views and opinions presented herein are those of the author and do not necessarily represent the views of DoD or the Army. Appearance of, or reference to, any commercial products or services does not constitute DoD or Army endorsement of those products or services. The appearance of external hyperlinks does not constitute DoD or Army endorsement of the linked websites, or the information, products or services therein.

# Agenda

- Cyber Threats in the News
- Defining Cyber Threat Intelligence (CTI)
- CTI Terminology
- CTI Technical Analysis
- MITRE ATT@CK – Enterprise
- Search Engine Optimization (SEO) Poisoning – Technique Overview
- Volt Typhoon – Campaign Overview
- Applying Army Doctrine to Cyberspace to Mitigate Organizational Risk
- Closing Remarks

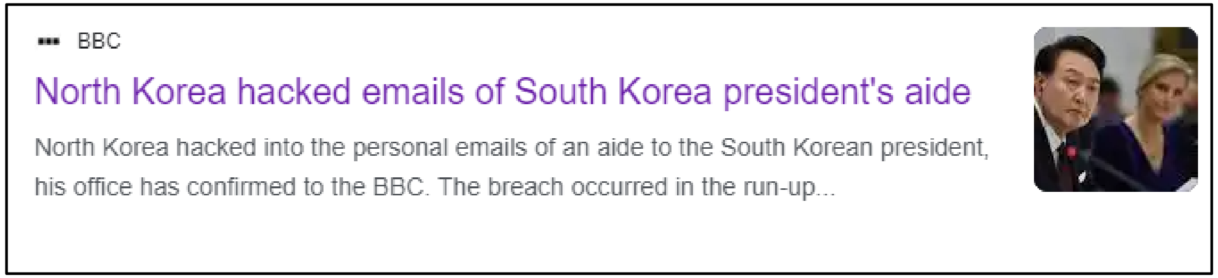
# Cyber Threats in the News



WSJ WSJ

FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale

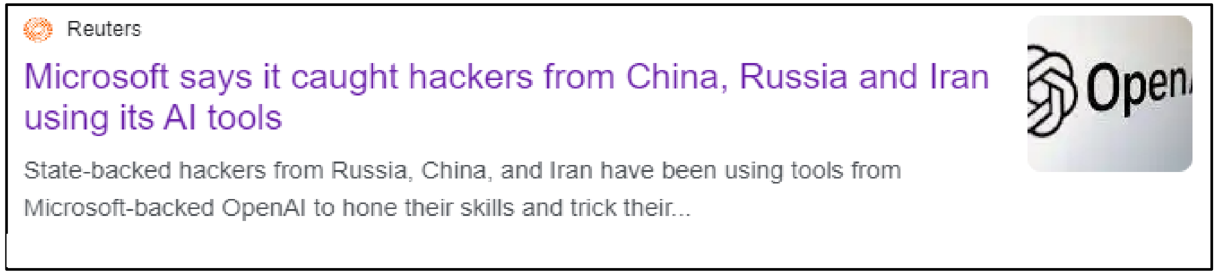
Christopher Wray warns that pre-positioned malware could be triggered to disrupt critical systems in the U.S..



BBC

North Korea hacked emails of South Korea president's aide

North Korea hacked into the personal emails of an aide to the South Korean president, his office has confirmed to the BBC. The breach occurred in the run-up...



Reuters

Microsoft says it caught hackers from China, Russia and Iran using its AI tools

State-backed hackers from Russia, China, and Iran have been using tools from Microsoft-backed OpenAI to hone their skills and trick their...

# Defining Cyber Threat Intelligence (CTI)

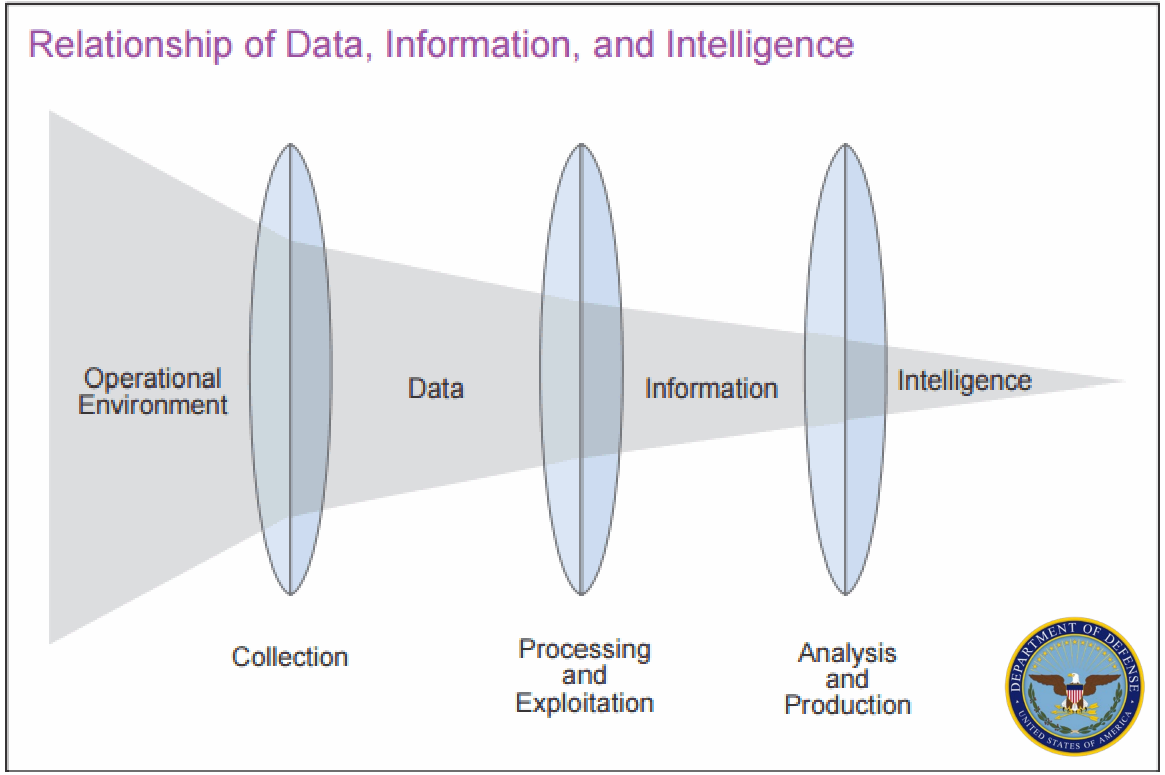
Analyzed information about the hostile intent, opportunity, and capability of an adversary that satisfies a requirement. SANS

**Threat + Vulnerability + Impact** = **Risk**

Adversary Capability & Intent

System Weaknesses

Operational Impairment to a CDR's Mission



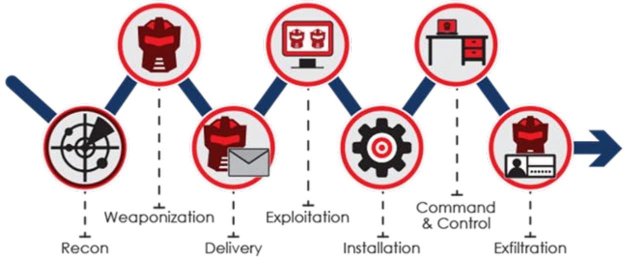
# CTI Terminology

- Adversary / Threat
- Intelligence Requirement
- Intrusion
- Activity Group
- Threat Actor
- Campaign
- Advanced Persistent Threat
- Target vs. Victim
- Persona
- Tactic, Technique, Procedure (TTP)
- Tradecraft
- Indicator

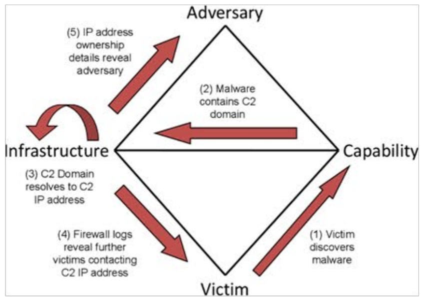
# CTI Technical Analysis

We use structured analytic techniques to analyze activity on the DoDIN to provide meaningful information to support leadership decisions, defenders' needs, and Intelligence efforts.

KILL CHAIN



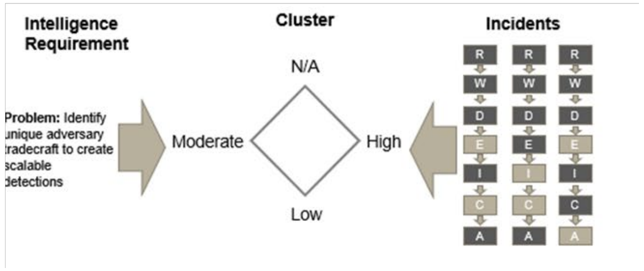
DIAMOND MODEL


Adversary
(5) IP address ownership details reveal adversary
(2) Malware contains C2 domain
Infrastructure
Capability
(3) C2 Domain resolves to C2 IP address
(4) Firewall logs reveal further victims contacting C2 IP address
(1) Victim discovers malware
Victim

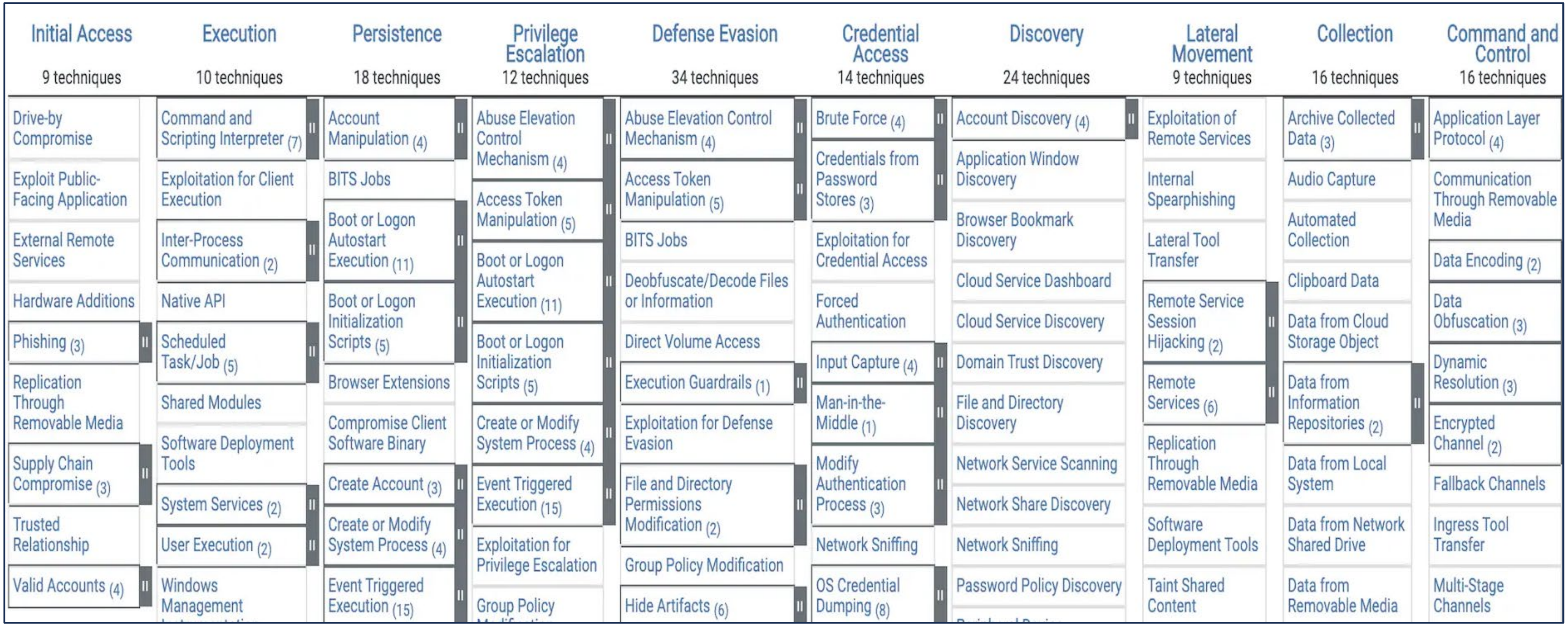
ATT&CK FRAMEWORK

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command And Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 items | 27 items | 42 items | 21 items | 67 items | 16 items | 22 items | 15 items | 13 items | 21 items | 9 items | 14 items |

CTI Analysis


Intelligence Requirement
Cluster
Incidents
N/A
Problem: Identify unique adversary tradecraft to create scalable detections
Moderate
High
Low
R
W
D
E
I
C
A

# MITRE ATT@CK – Enterprise



| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control |
|---|---|---|---|---|---|---|---|---|---|
| 9 techniques | 10 techniques | 18 techniques | 12 techniques | 34 techniques | 14 techniques | 24 techniques | 9 techniques | 16 techniques | 16 techniques |
| Drive-by Compromise | Command and Scripting Interpreter (7) | Account Manipulation (4) | Abuse Elevation Control Mechanism (4) | Abuse Elevation Control Mechanism (4) | Brute Force (4) | Account Discovery (4) | Exploitation of Remote Services | Archive Collected Data (3) | Application Layer Protocol (4) |
| Exploit Public-Facing Application | Exploitation for Client Execution | BITS Jobs | Access Token Manipulation (5) | Access Token Manipulation (5) | Credentials from Password Stores (3) | Application Window Discovery | Internal Spearphishing | Audio Capture | Communication Through Removable Media |
| External Remote Services | Inter-Process Communication (2) | Boot or Logon Autostart Execution (11) | Boot or Logon Autostart Execution (11) | BITS Jobs | Exploitation for Credential Access | Browser Bookmark Discovery | Lateral Tool Transfer | Automated Collection | Data Encoding (2) |
| Hardware Additions | Native API | Boot or Logon Initialization Scripts (5) | Boot or Logon Initialization Scripts (5) | Deobfuscate/Decode Files or Information | Forced Authentication | Cloud Service Dashboard | Remote Service Session Hijacking (2) | Clipboard Data | Data Obfuscation (3) |
| Phishing (3) | Scheduled Task/Job (5) | Browser Extensions | Create or Modify System Process (4) | Direct Volume Access | Input Capture (4) | Cloud Service Discovery | Remote Services (6) | Data from Cloud Storage Object | Dynamic Resolution (3) |
| Replication Through Removable Media | Shared Modules | Compromise Client Software Binary | Event Triggered Execution (15) | Execution Guardrails (1) | Man-in-the-Middle (1) | Domain Trust Discovery | Replication Through Removable Media | Data from Information Repositories (2) | Encrypted Channel (2) |
| Supply Chain Compromise (3) | Software Deployment Tools | Create Account (3) | Exploitation for Privilege Escalation | Exploitation for Defense Evasion | Modify Authentication Process (3) | File and Directory Discovery | Software Deployment Tools | Data from Local System | Fallback Channels |
| Trusted Relationship | System Services (2) | Create or Modify System Process (4) | Group Policy | File and Directory Permissions Modification (2) | Network Sniffing | Network Service Scanning | Taint Shared Content | Data from Network Shared Drive | Ingress Tool Transfer |
| Valid Accounts (4) | User Execution (2) | Event Triggered Execution (15) | | Group Policy Modification | OS Credential Dumping (8) | Network Share Discovery | | Data from Removable Media | Multi-Stage Channels |
| | Windows Management | | | Hide Artifacts (6) | | Network Sniffing | | | |
| | | | | | | Password Policy Discovery | | | |

# SEO Poisoning – Technique Overview

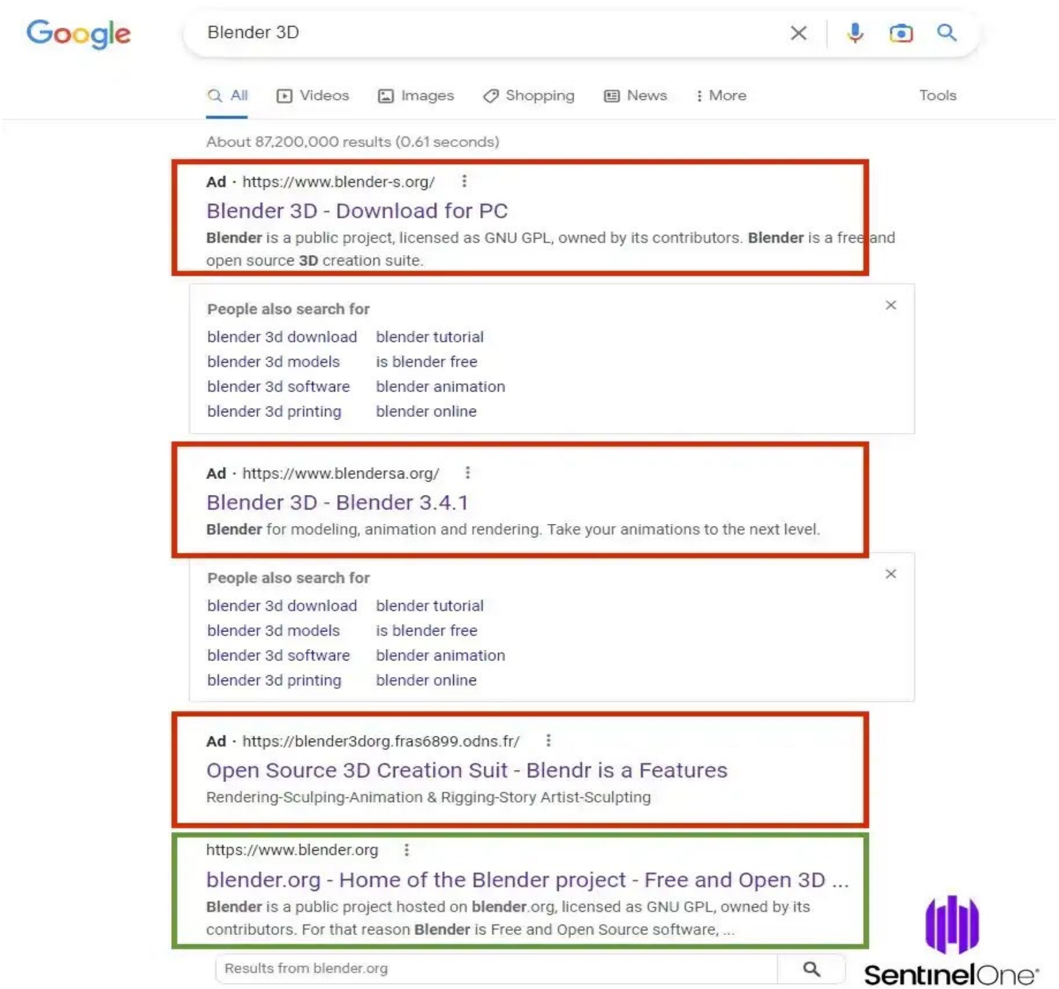
The best places to hide a dead body
is page 2 of Google search results.
- Unknown.

# SEO Poisoning

The above three malicious ads link to:

- blender-s.org
- blendersa.org
- blender3dorg.fras6899.odns.fr

The top results, blender-s.org is a near exact copy of the legitimate Blender domain.



About 87,200,000 results (0.61 seconds)

**Ad** · https://www.blender-s.org/

Blender 3D - Download for PC

**Blender** is a public project, licensed as GNU GPL, owned by its contributors. **Blender** is a free and open source **3D** creation suite.

People also search for

blender 3d download | blender tutorial
blender 3d models | is blender free
blender 3d software | blender animation
blender 3d printing | blender online

**Ad** · https://www.blendersa.org/

Blender 3D - Blender 3.4.1

**Blender** for modeling, animation and rendering. Take your animations to the next level.

People also search for

blender 3d download | blender tutorial
blender 3d models | is blender free
blender 3d software | blender animation
blender 3d printing | blender online

**Ad** · https://blender3dorg.fras6899.odns.fr/

Open Source 3D Creation Suit - Blendr is a Features

Rendering-Sculping-Animation & Rigging-Story Artist-Sculpting

https://www.blender.org

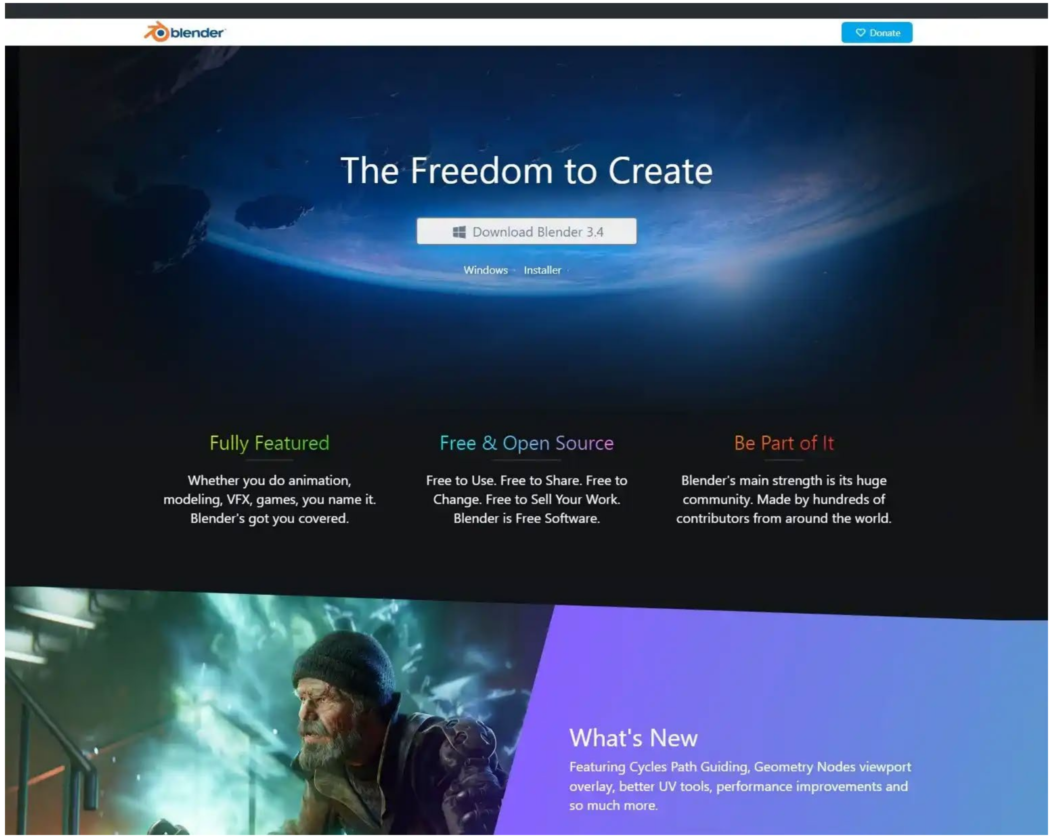
blender.org - Home of the Blender project - Free and Open 3D ...

**Blender** is a public project hosted on **blender**.org, licensed as GNU GPL, owned by its contributors. For that reason **Blender** is Free and Open Source software, ...

Results from blender.org

SentinelOne

# SEO Poisoning



The Freedom to Create

Fully Featured

Whether you do animation, modeling, VFX, games, you name it. Blender's got you covered.

Free & Open Source

Free to Use. Free to Share. Free to Change. Free to Sell Your Work. Blender is Free Software.

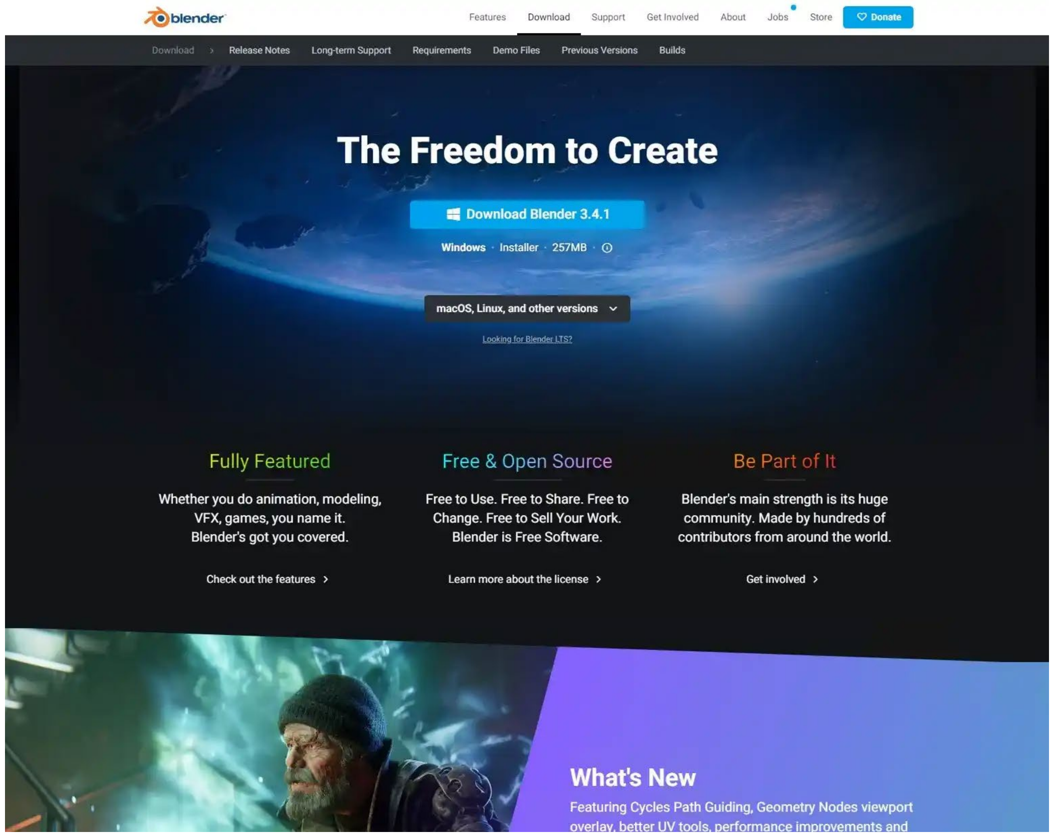
Be Part of It

Blender's main strength is its huge community. Made by hundreds of contributors from around the world.

What's New

Featuring Cycles Path Guiding, Geometry Nodes viewport overlay, better UV tools, performance improvements and so much more.

Malicious Website



The Freedom to Create

Fully Featured

Whether you do animation, modeling, VFX, games, you name it. Blender's got you covered.

Free & Open Source

Free to Use. Free to Share. Free to Change. Free to Sell Your Work. Blender is Free Software.

Be Part of It

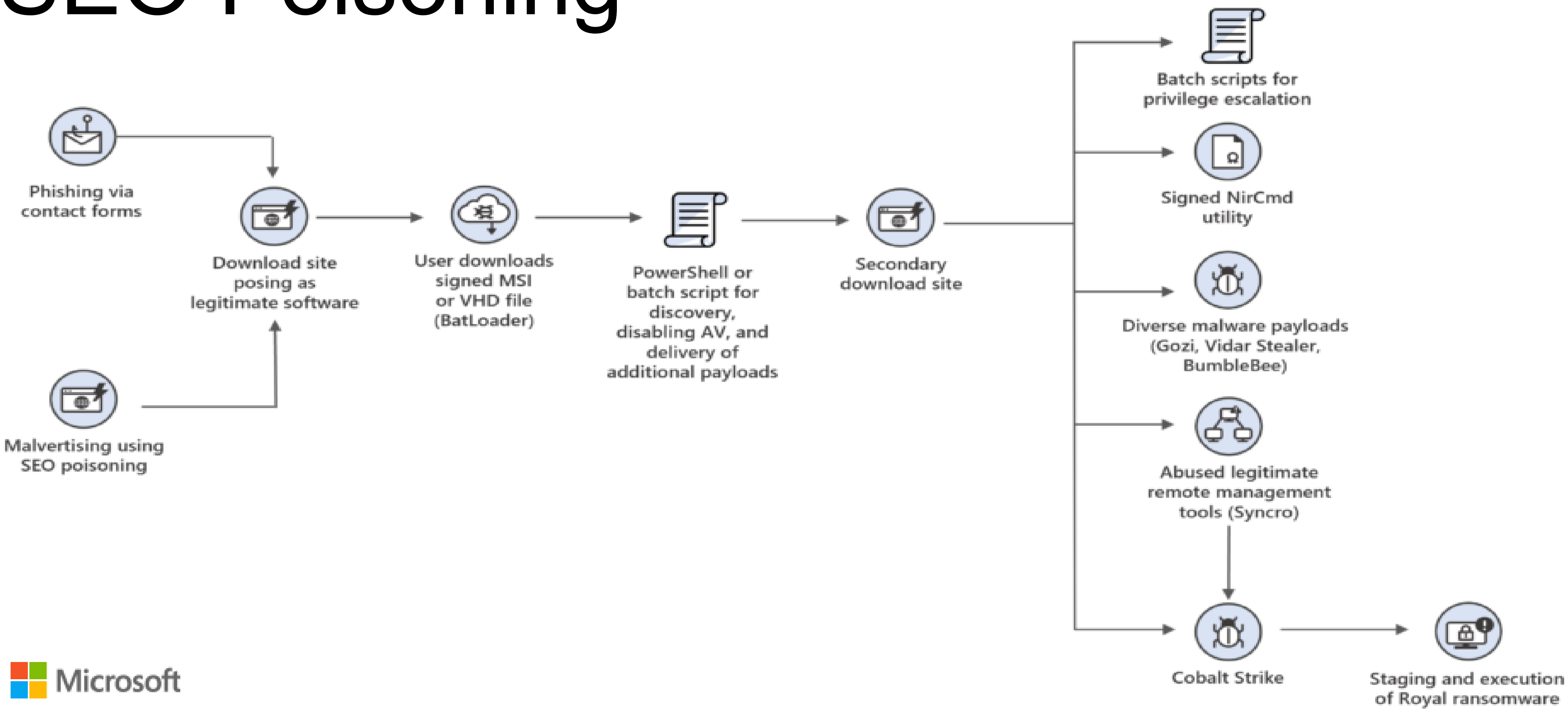
Blender's main strength is its huge community. Made by hundreds of contributors from around the world.

What's New

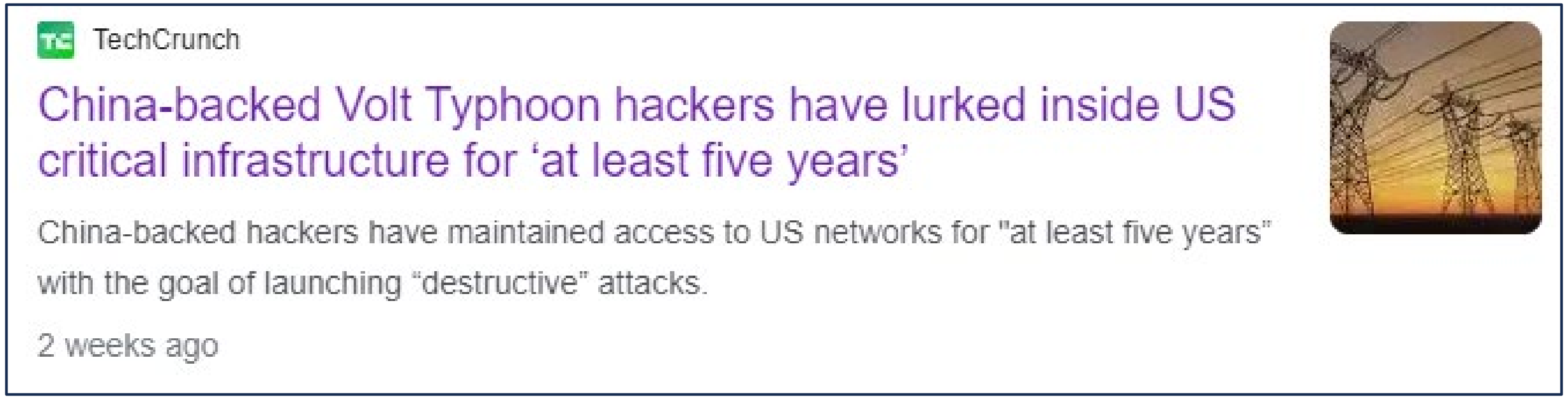
Featuring Cycles Path Guiding, Geometry Nodes viewport overlay, better UV tools, performance improvements and

Legitimate Website

# SEO Poisoning


Phishing via contact forms
Download site posing as legitimate software
Malvertising using SEO poisoning
User downloads signed MSI or VHD file (BatLoader)
PowerShell or batch script for discovery, disabling AV, and delivery of additional payloads
Secondary download site
Batch scripts for privilege escalation
Signed NirCmd utility
Diverse malware payloads (Gozi, Vidar Stealer, BumbleBee)
Abused legitimate remote management tools (Syncro)
Cobalt Strike
Staging and execution of Royal ransomware
Microsoft

# Volt Typhoon – Campaign Overview



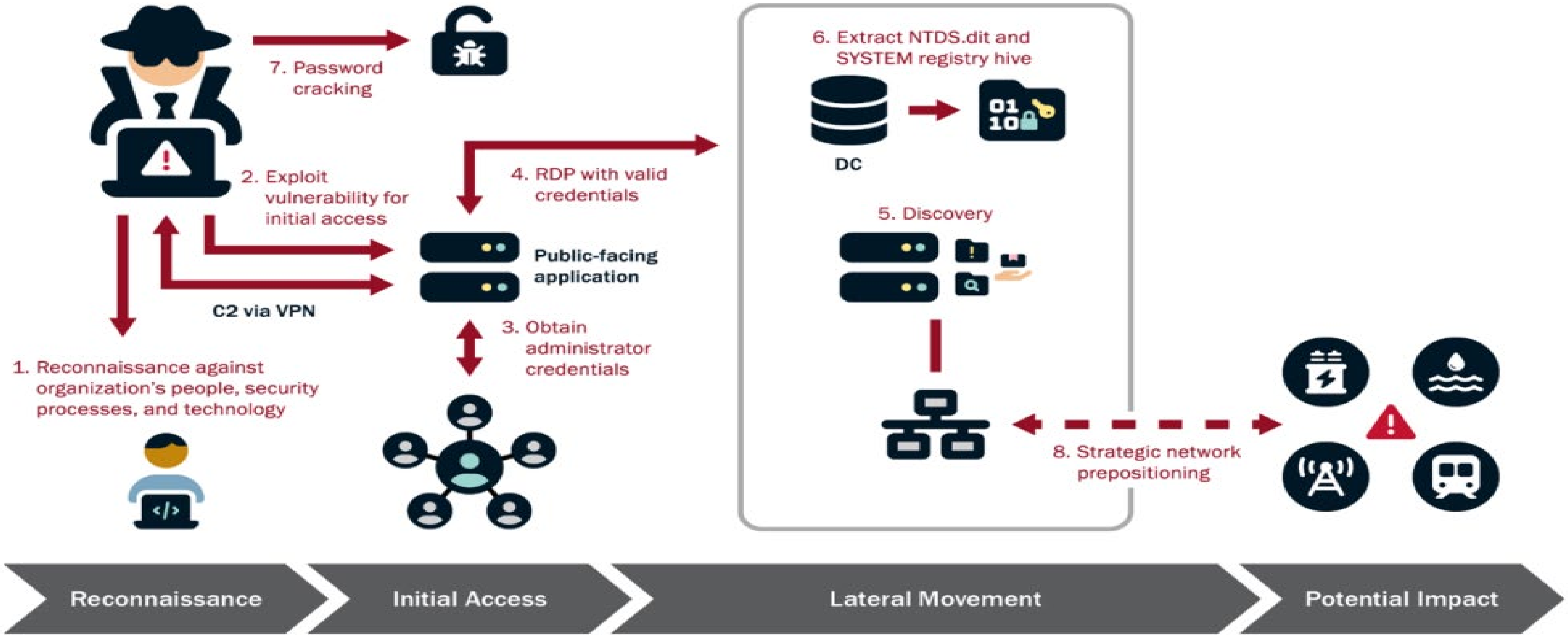
TechCrunch

China-backed Volt Typhoon hackers have lurked inside US critical infrastructure for ‘at least five years’

China-backed hackers have maintained access to US networks for "at least five years" with the goal of launching “destructive” attacks.

2 weeks ago

# Volt Typhoon – Typical Activity



7. Password cracking

2. Exploit vulnerability for initial access

C2 via VPN

4. RDP with valid credentials

Public-facing application

3. Obtain administrator credentials

1. Reconnaissance against organization's people, security processes, and technology

6. Extract NTDS.dit and SYSTEM registry hive

DC

5. Discovery

8. Strategic network prepositioning

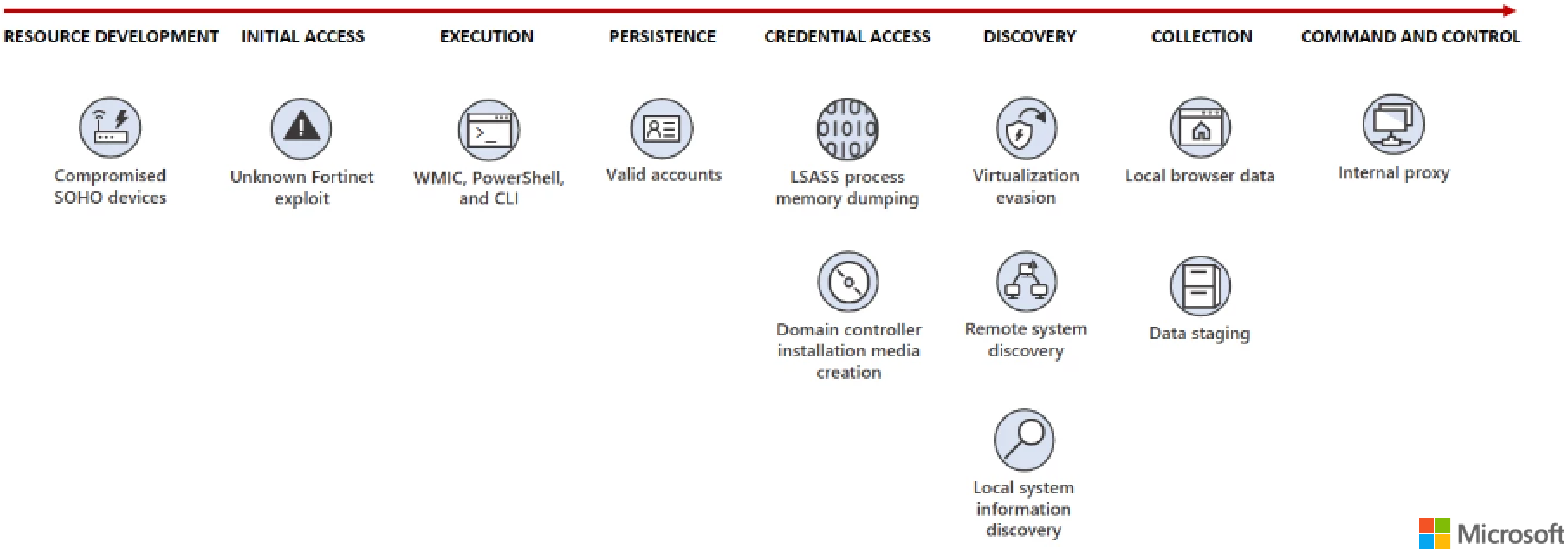
Reconnaissance

Initial Access

Lateral Movement

Potential Impact

# Volt Typhoon – Attack Diagram



RESOURCE DEVELOPMENT

Compromised SOHO devices

INITIAL ACCESS

Unknown Fortinet exploit

EXECUTION

WMIC, PowerShell, and CLI

PERSISTENCE

Valid accounts

CREDENTIAL ACCESS

LSASS process memory dumping

Domain controller installation media creation

DISCOVERY

Virtualization evasion

Remote system discovery

Local system information discovery

COLLECTION

Local browser data

Data staging

COMMAND AND CONTROL

Internal proxy

Microsoft

# Applying Army Doctrine to Mitigate Organizational Risk

# Traditional Battlefields

## SUPPORT ZONE (SZ)

*Designed to be free of significant enemy action and permit effective logistics and administration .*

- Camouflage, Concealment, Cover, and Deception measures to protect from precision attack
- A sanctuary that is noncontiguous with other zones in the AOR

## BATTLE ZONE (BZ)

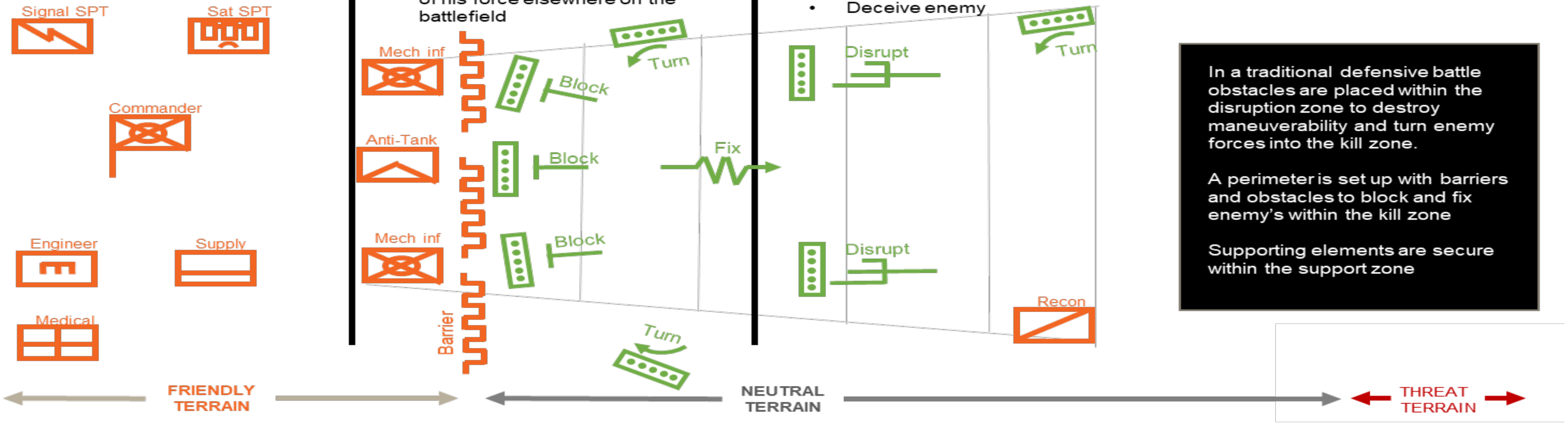
*Conduct decisive actions to exploit opportunities created by actions in the disruption zone.*

- Draw enemy attention and resources to action
- Hold terrain
- Inflict casualties on vulnerable enemy units
- Prevent enemy from moving a part of his force elsewhere on the battlefield

## DISRUPTION ZONE (DZ)

*Area in which the unit's disruption force will conduct disruption task to set conditions for successful combat actions by fixing enemy forces and placing fire on them.*

- Attack enemy's engineer elements to destroy maneuverability in complex terrain.
- Strip away enemy's reconnaissance and deny him the ability to acquire and engage
- Disrupt offensive preparation
- Gaining and maintaining reconnaissance contact with key enemy elements
- Deceive enemy

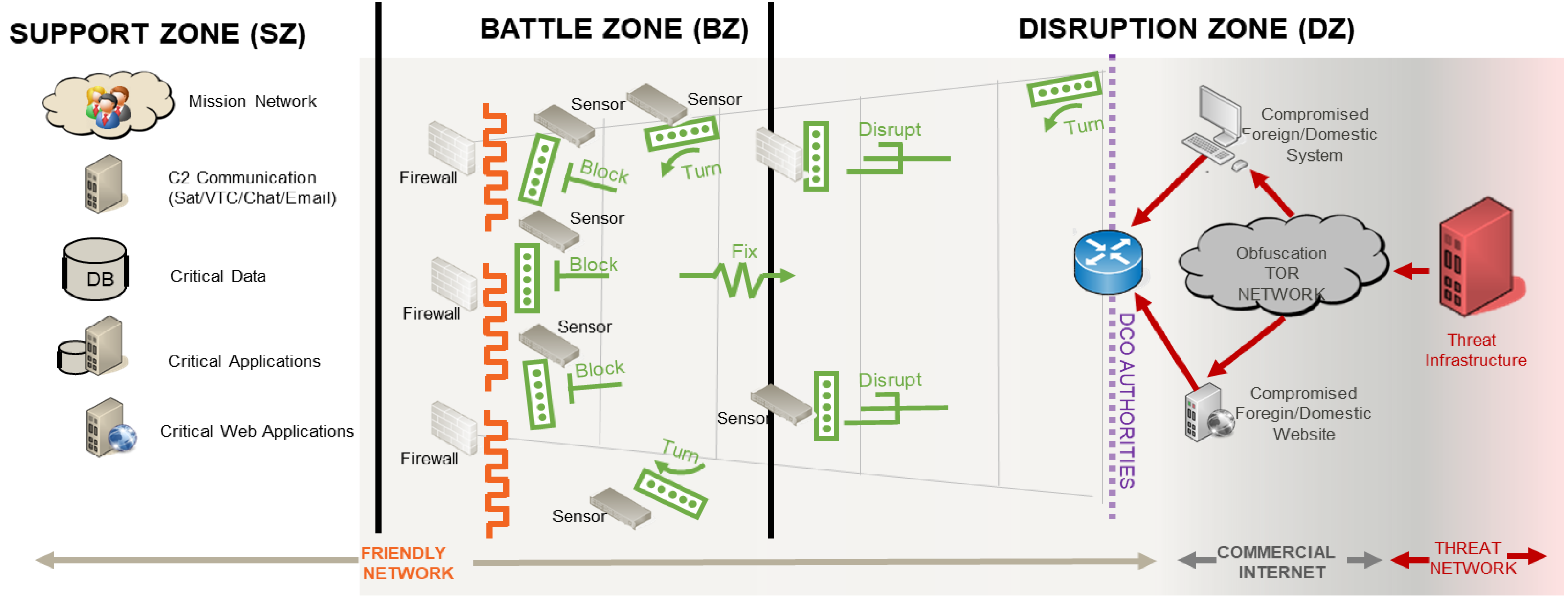


In a traditional defensive battle obstacles are placed within the disruption zone to destroy maneuverability and turn enemy forces into the kill zone.

A perimeter is set up with barriers and obstacles to block and fix enemy's within the kill zone

Supporting elements are secure within the support zone

# A Theoretical Battlefield in Cyberspace



# Closing Remarks