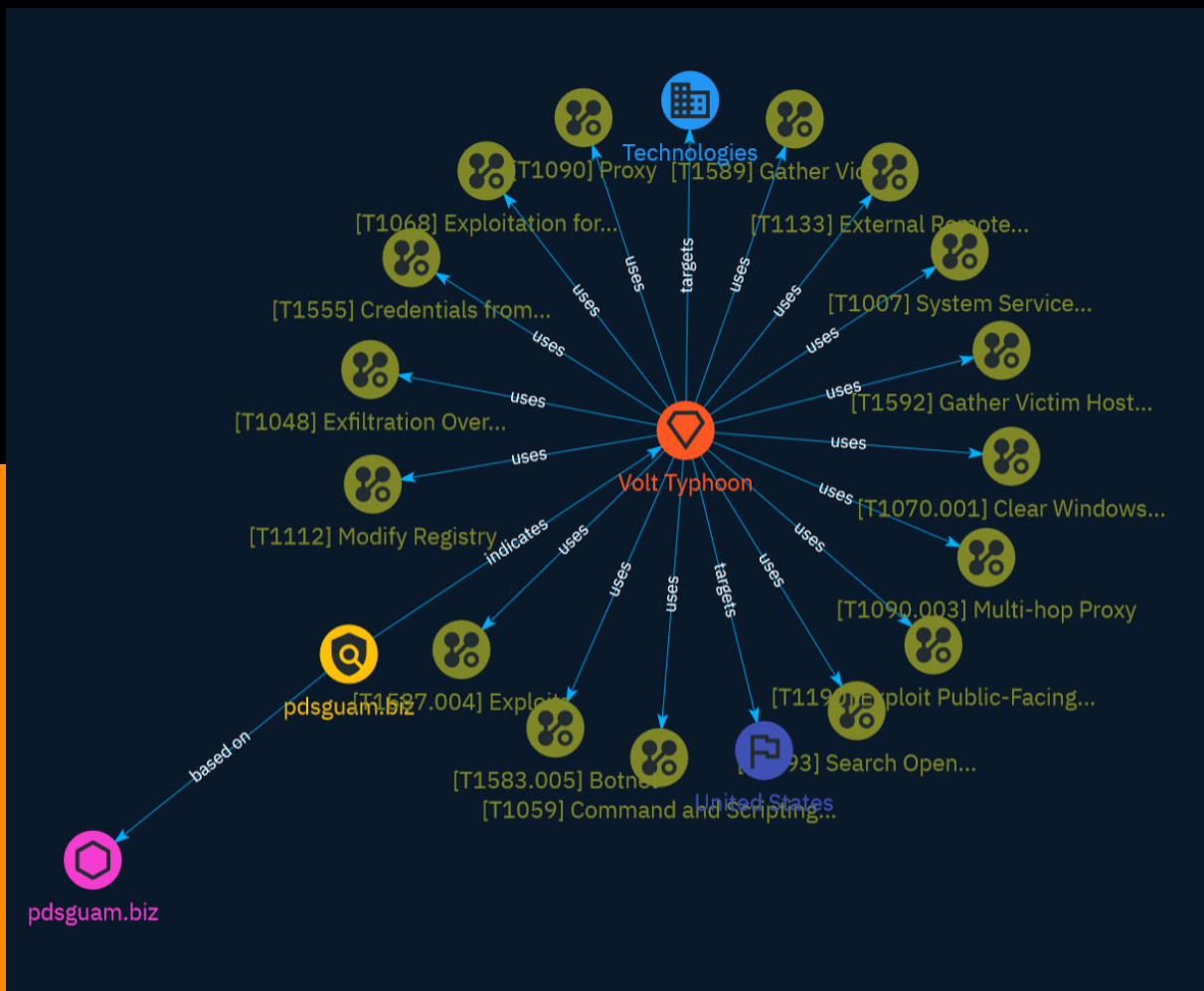


# NETMANAGEIT

## Intelligence Report

# PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure



# Table of contents

---

## Overview

---

● Description	4
● Confidence	4
● Content	5

---

## Entities

---

● Indicator	6
● Intrusion-Set	7
● Attack-Pattern	8
● Country	31
● Sector	32

---

## Observables

---

● Domain-Name	33
---------------	----



## External References

- External References

34

# Overview

## Description

This report provides analysis of three files obtained from critical infrastructure compromised by Chinese state-sponsored threat actor Volt Typhoon. The files enable command-and-control and discovery capabilities. Volt Typhoon is known to target US critical infrastructure. The report provides technical analysis of the files, including tags, relationships between files and command-and-control infrastructure, and recommendations for defense.

## Confidence

*This value represents the confidence in the correctness of the data contained within this report.*

15 / 100

# Content

N/A

# Indicator

**Name**

pdsguam.biz

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'pdsguam.biz']

**Name**

pdsguam.biz

**Pattern Type**

stix

**Pattern**

[domain-name:value = 'pdsguam.biz']

# Intrusion-Set

## Name

Volt Typhoon

## Description

[Volt Typhoon](<https://attack.mitre.org/groups/G1017>) is a People's Republic of China (PRC) state-sponsored actor that has been active since at least 2021. [Volt Typhoon](<https://attack.mitre.org/groups/G1017>) typically focuses on espionage and information gathering and has targeted critical infrastructure organizations in the US including Guam. [Volt Typhoon](<https://attack.mitre.org/groups/G1017>) has emphasized stealth in operations using web shells, living-off-the-land (LOTL) binaries, hands on keyboard activities, and stolen credentials.(Citation: Microsoft Volt Typhoon May 2023)(Citation: Joint Cybersecurity Advisory Volt Typhoon June 2023)(Citation: Secureworks BRONZE SILHOUETTE May 2023)

## Name

Volt Typhoon

## Description

[Volt Typhoon](<https://attack.mitre.org/groups/G1017>) is a People's Republic of China (PRC) state-sponsored actor that has been active since at least 2021. [Volt Typhoon](<https://attack.mitre.org/groups/G1017>) typically focuses on espionage and information gathering and has targeted critical infrastructure organizations in the US including Guam. [Volt Typhoon](<https://attack.mitre.org/groups/G1017>) has emphasized stealth in operations using web shells, living-off-the-land (LOTL) binaries, hands on keyboard activities, and stolen credentials.(Citation: Microsoft Volt Typhoon May 2023)(Citation: Joint Cybersecurity Advisory Volt Typhoon June 2023)(Citation: Secureworks BRONZE SILHOUETTE May 2023)

# Attack-Pattern

Name
Exploits
ID
T1587.004
Description



Adversaries may develop exploits that can be used during targeting. An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. Rather than finding/modifying exploits from online or purchasing them from exploit vendors, an adversary may develop their own exploits.(Citation: NYTStuxnet) Adversaries may use information acquired via [Vulnerabilities](<https://attack.mitre.org/techniques/T1588/006>) to focus exploit development efforts. As part of the exploit development process, adversaries may uncover exploitable vulnerabilities through methods such as fuzzing and patch analysis.(Citation: Irongeek Sims BSides 2017) As with legitimate development efforts, different skill sets may be required for developing exploits. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's exploit development capabilities, provided the adversary plays a role in shaping requirements and maintains an initial degree of exclusivity to the exploit. Adversaries may use exploits during various phases of the adversary lifecycle (i.e. [Exploit Public-Facing Application](<https://attack.mitre.org/techniques/T1190>), [Exploitation for Client Execution](<https://attack.mitre.org/techniques/T1203>), [Exploitation for Privilege Escalation](<https://attack.mitre.org/techniques/T1068>), [Exploitation for Defense Evasion](<https://attack.mitre.org/techniques/T1211>), [Exploitation for Credential Access](<https://attack.mitre.org/techniques/T1212>), [Exploitation of Remote Services](<https://attack.mitre.org/techniques/T1210>), and [Application or System Exploitation](<https://attack.mitre.org/techniques/T1499/004>)).

**Name**

Exploitation for Privilege Escalation

**ID**

T1068

**Description**

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing

certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD). (Citation: ESET InvisiMole June 2020) (Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer] (<https://attack.mitre.org/techniques/T1105>) or [Lateral Tool Transfer] (<https://attack.mitre.org/techniques/T1570>).

**Name**

Multi-hop Proxy

**ID**

T1090.003

**Description**

To disguise the source of malicious traffic, adversaries may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source. A particular variant of this behavior is to use onion routing networks, such as the publicly available TOR network. (Citation: Onion Routing) In the case of network infrastructure, particularly routers, it is possible for an adversary to leverage multiple compromised devices to create a multi-hop proxy chain within the Wide-Area Network (WAN) of the enterprise. By leveraging [Patch System Image] (<https://attack.mitre.org/techniques/T1601/001>), adversaries can add custom code to the affected network devices that will implement onion routing between those nodes. This custom onion routing network will transport the encrypted C2 traffic through the compromised population, allowing adversaries to communicate with any device within the onion routing network. This method is dependent upon the [Network Boundary Bridging]

(<https://attack.mitre.org/techniques/T1599>) method in order to allow the adversaries to cross the protected network boundary of the Internet perimeter and into the organization's WAN. Protocols such as ICMP may be used as a transport.

**Name**

Exfiltration Over Alternative Protocol

**ID**

T1048

**Description**

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels. [Exfiltration Over Alternative Protocol](<https://attack.mitre.org/techniques/T1048>) can be done using various common operating system utilities such as [Net](<https://attack.mitre.org/software/S0039>)/SMB or FTP.(Citation: Palo Alto OilRig Oct 2016) On macOS and Linux `curl` may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.(Citation: 20 macOS Common Tools and Techniques) Many IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3) support the direct download of files, emails, source code, and other sensitive information via the web console or [Cloud API](<https://attack.mitre.org/techniques/T1059/009>).

**Name**

Search Open Websites/Domains

**ID**

T1593

**Description**

Adversaries may search freely available websites and/or domains for information about victims that can be used during targeting. Information about victims may be available in various online sites, such as social media, new sites, or those hosting information about business operations such as hiring or requested/rewarded contracts.(Citation: Cyware Social Media)(Citation: SecurityTrails Google Hacking)(Citation: ExploitDB GoogleHacking) Adversaries may search in different online sites depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Phishing](https://attack.mitre.org/techniques/T1566)).

**Name**

Command and Scripting Interpreter

**ID**

T1059

**Description**

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote

Services](<https://attack.mitre.org/techniques/T1021>) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

**Name**

Proxy

**ID**

T1090

**Description**

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](<https://attack.mitre.org/software/S0040>), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

**Name**

Clear Windows Event Logs

**ID**

T1070.001

**Description**

Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alerts and notifications. There are three system-

defined sources of events: System, Application, and Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit. The event logs can be cleared with the following utility commands: \* `wevtutil cl system` \* `wevtutil cl application` \* `wevtutil cl security` These logs may also be cleared through other mechanisms, such as the event viewer GUI or [PowerShell](https://attack.mitre.org/techniques/T1059/001). For example, adversaries may use the PowerShell command `Remove-EventLog -LogName Security` to delete the Security EventLog and after reboot, disable future logging. Note: events may still be generated and logged in the .evtx file between the time the command is run and the reboot.(Citation: disable\_win\_evt\_logging)

**Name**

Modify Registry

**ID**

T1112

**Description**

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

**Name**

## Gather Victim Identity Information

**ID**

T1589

**Description**

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](<https://attack.mitre.org/techniques/T1598>). Information about users could also be enumerated via other active means (i.e. [Active Scanning](<https://attack.mitre.org/techniques/T1595>)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. (Citation: GrimBlog UsernameEnum) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](<https://attack.mitre.org/techniques/T1593/001>) or [Search Victim-Owned Websites](<https://attack.mitre.org/techniques/T1594>)).(Citation: OPM Leak)(Citation: Register Deloitte) (Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds) (Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](<https://attack.mitre.org/techniques/T1593>) or [Phishing for Information](<https://attack.mitre.org/techniques/T1598>)), establishing operational resources (ex: [Compromise Accounts](<https://attack.mitre.org/techniques/T1586>)), and/or initial access (ex: [Phishing](<https://attack.mitre.org/techniques/T1566>) or [Valid Accounts](<https://attack.mitre.org/techniques/T1078>)).

**Name**

Exploit Public-Facing Application

**ID**

T1190

**Description**

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion] (<https://attack.mitre.org/techniques/T1211>). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](<https://attack.mitre.org/techniques/T1611>), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

**Name**

Credentials from Password Stores

**ID**

T1555

**Description**

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

**Name**



## System Service Discovery

**ID**

T1007

**Description**

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as `sc query`, `tasklist /svc`, `systemctl --type=service`, and `net start`. Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

**Name**

Botnet

**ID**

T1583.005

**Description**

Adversaries may buy, lease, or rent a network of compromised systems that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Adversaries may purchase a subscription to use an existing botnet from a booter/stresser service. With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing](https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS). (Citation: Imperva DDoS for Hire)(Citation: Krebs-Anna)(Citation: Krebs-Bazaar)(Citation: Krebs-Booter)

**Name**

## External Remote Services

**ID**

T1133

**Description**

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management] (<https://attack.mitre.org/techniques/T1021/006>) and [VNC](<https://attack.mitre.org/techniques/T1021/005>) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](<https://attack.mitre.org/techniques/T1078>) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

**Name**

Gather Victim Host Information

**ID**

T1592

**Description**

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding

its configuration (ex: operating system, language, etc.). Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](<https://attack.mitre.org/techniques/T1595>) or [Phishing for Information](<https://attack.mitre.org/techniques/T1598>). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](<https://attack.mitre.org/techniques/T1593/001>) or [Search Victim-Owned Websites](<https://attack.mitre.org/techniques/T1594>)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](<https://attack.mitre.org/techniques/T1593>) or [Search Open Technical Databases](<https://attack.mitre.org/techniques/T1596>)), establishing operational resources (ex: [Develop Capabilities](<https://attack.mitre.org/techniques/T1587>) or [Obtain Capabilities](<https://attack.mitre.org/techniques/T1588>)), and/or initial access (ex: [Supply Chain Compromise](<https://attack.mitre.org/techniques/T1195>) or [External Remote Services](<https://attack.mitre.org/techniques/T1133>)).

**Name**

Exploits

**ID**

T1587.004

**Description**

Adversaries may develop exploits that can be used during targeting. An exploit takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer hardware or software. Rather than finding/modifying exploits from online or purchasing them from exploit vendors, an adversary may develop their own exploits.(Citation: NYTStuxnet) Adversaries may use information acquired via [Vulnerabilities](<https://attack.mitre.org/techniques/T1588/006>) to focus exploit development efforts. As part of the exploit development process, adversaries may uncover exploitable vulnerabilities through methods such as fuzzing and patch analysis.(Citation: Irongeek Sims BSides 2017) As with legitimate development efforts, different skill sets may be required for developing exploits. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's exploit development capabilities, provided the adversary plays a role in shaping requirements and maintains an initial degree of exclusivity to the exploit. Adversaries may use exploits during various phases of the adversary lifecycle (i.e. [Exploit Public-Facing Application](<https://attack.mitre.org/techniques/T1190>), [Exploitation for

Client Execution](<https://attack.mitre.org/techniques/T1203>), [Exploitation for Privilege Escalation](<https://attack.mitre.org/techniques/T1068>), [Exploitation for Defense Evasion](<https://attack.mitre.org/techniques/T1211>), [Exploitation for Credential Access](<https://attack.mitre.org/techniques/T1212>), [Exploitation of Remote Services](<https://attack.mitre.org/techniques/T1210>), and [Application or System Exploitation](<https://attack.mitre.org/techniques/T1499/004>)).

**Name**

Exploitation for Privilege Escalation

**ID**

T1068

**Description**

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](<https://attack.mitre.org/techniques/T1105>) or [Lateral Tool Transfer](<https://attack.mitre.org/techniques/T1570>).

**Name**

Multi-hop Proxy

**ID**

T1090.003

**Description**

To disguise the source of malicious traffic, adversaries may chain together multiple proxies. Typically, a defender will be able to identify the last proxy traffic traversed before it enters their network; the defender may or may not be able to identify any previous proxies before the last-hop proxy. This technique makes identifying the original source of the malicious traffic even more difficult by requiring the defender to trace malicious traffic through several proxies to identify its source. A particular variant of this behavior is to use onion routing networks, such as the publicly available TOR network. (Citation: Onion Routing) In the case of network infrastructure, particularly routers, it is possible for an adversary to leverage multiple compromised devices to create a multi-hop proxy chain within the Wide-Area Network (WAN) of the enterprise. By leveraging [Patch System Image] (<https://attack.mitre.org/techniques/T1601/001>), adversaries can add custom code to the affected network devices that will implement onion routing between those nodes. This custom onion routing network will transport the encrypted C2 traffic through the compromised population, allowing adversaries to communicate with any device within the onion routing network. This method is dependent upon the [Network Boundary Bridging] (<https://attack.mitre.org/techniques/T1599>) method in order to allow the adversaries to cross the protected network boundary of the Internet perimeter and into the organization's WAN. Protocols such as ICMP may be used as a transport.

**Name**

Exfiltration Over Alternative Protocol

**ID**

T1048

**Description**

Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels. [Exfiltration Over Alternative Protocol](<https://attack.mitre.org/techniques/T1048>) can be done using various common operating system utilities such as [Net](<https://attack.mitre.org/software/S0039>)/SMB or FTP.(Citation: Palo Alto OilRig Oct 2016) On macOS and Linux `curl` may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.(Citation: 20 macOS Common Tools and Techniques) Many IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3) support the direct download of files, emails, source code, and other sensitive information via the web console or [Cloud API](<https://attack.mitre.org/techniques/T1059/009>).

**Name**

Search Open Websites/Domains

**ID**

T1593

**Description**

Adversaries may search freely available websites and/or domains for information about victims that can be used during targeting. Information about victims may be available in various online sites, such as social media, news sites, or those hosting information about business operations such as hiring or requested/rewarded contracts.(Citation: Cyware Social Media)(Citation: SecurityTrails Google Hacking)(Citation: ExploitDB GoogleHacking) Adversaries may search in different online sites depending on what information they seek to gather. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](<https://attack.mitre.org/techniques/T1598>) or [Search Open Technical Databases](<https://attack.mitre.org/techniques/T1596>)), establishing operational resources (ex: [Establish Accounts](<https://attack.mitre.org/techniques/T1585>) or [Compromise Accounts](<https://attack.mitre.org/techniques/T1586>)), and/or initial access (ex: [External Remote Services](<https://attack.mitre.org/techniques/T1133>) or [Phishing](<https://attack.mitre.org/techniques/T1566>)).

**Name**

Command and Scripting Interpreter

**ID**

T1059

**Description**

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](<https://attack.mitre.org/techniques/T1059/004>) while Windows installations include the [Windows Command Shell](<https://attack.mitre.org/techniques/T1059/003>) and [PowerShell](<https://attack.mitre.org/techniques/T1059/001>). There are also cross-platform interpreters such as [Python](<https://attack.mitre.org/techniques/T1059/006>), as well as those commonly associated with client applications such as [JavaScript](<https://attack.mitre.org/techniques/T1059/007>) and [Visual Basic](<https://attack.mitre.org/techniques/T1059/005>). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](<https://attack.mitre.org/tactics/TA0001>) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](<https://attack.mitre.org/techniques/T1021>) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

**Name**

Proxy

**ID**

T1090

**Description**

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

**Name**

Clear Windows Event Logs

**ID**

T1070.001

**Description**

Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alerts and notifications. There are three system-defined sources of events: System, Application, and Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit. The event logs can be cleared with the following utility commands: \* ``wevtutil cl system`` \* ``wevtutil cl application`` \* ``wevtutil cl security`` These logs may also be cleared through other mechanisms, such as the event viewer GUI or [PowerShell](https://attack.mitre.org/techniques/T1059/001). For example, adversaries may use the PowerShell command ``Remove-EventLog -LogName Security`` to delete the Security EventLog and after reboot, disable future logging. Note: events may still be generated and logged in the .evtx file between the time the command is run and the reboot.(Citation: disable\_win\_evt\_logging)

**Name**



Modify Registry

**ID**

T1112

**Description**

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](<https://attack.mitre.org/software/S0075>) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](<https://attack.mitre.org/software/S0075>) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](<https://attack.mitre.org/techniques/T1078>) are required, along with access to the remote system's [SMB/Windows Admin Shares](<https://attack.mitre.org/techniques/T1021/002>) for RPC communication.

**Name**

Gather Victim Identity Information

**ID**

T1589

**Description**

Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](<https://attack.mitre.org/techniques/T1598>). Information about users could also be enumerated via other active means (i.e. [Active Scanning](<https://attack.mitre.org/techniques/T1595>)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. (Citation: GrimBlog UsernameEnum) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](<https://attack.mitre.org/techniques/T1593/001>) or [Search Victim-Owned Websites](<https://attack.mitre.org/techniques/T1594>)).(Citation: OPM Leak)(Citation: Register Deloitte)(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds)(Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](<https://attack.mitre.org/techniques/T1593>) or [Phishing for Information](<https://attack.mitre.org/techniques/T1598>)), establishing operational resources (ex: [Compromise Accounts](<https://attack.mitre.org/techniques/T1586>)), and/or initial access (ex: [Phishing](<https://attack.mitre.org/techniques/T1566>) or [Valid Accounts](<https://attack.mitre.org/techniques/T1078>)).

**Name**

Exploit Public-Facing Application

**ID**

T1190

**Description**

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion]

(<https://attack.mitre.org/techniques/T1211>). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](<https://attack.mitre.org/techniques/T1611>), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

**Name**

Credentials from Password Stores

**ID**

T1555

**Description**

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

**Name**

System Service Discovery

**ID**

T1007

**Description**

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as `sc query`, `tasklist /svc`, `systemctl --type=service`, and `net start`. Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

**Name**

Botnet

**ID**

T1583.005

**Description**

Adversaries may buy, lease, or rent a network of compromised systems that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated tasks.(Citation: Norton Botnet) Adversaries may purchase a subscription to use an existing botnet from a booter/stresser service. With a botnet at their disposal, adversaries may perform follow-on activity such as large-scale [Phishing](https://attack.mitre.org/techniques/T1566) or Distributed Denial of Service (DDoS). (Citation: Imperva DDoS for Hire)(Citation: Krebs-Anna)(Citation: Krebs-Bazaar)(Citation: Krebs-Booter)

**Name**

External Remote Services

**ID**

T1133

**Description**

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](<https://attack.mitre.org/techniques/T1021/006>) and [VNC](<https://attack.mitre.org/techniques/T1021/005>) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](<https://attack.mitre.org/techniques/T1078>) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

**Name**

Gather Victim Host Information

**ID**

T1592

**Description**

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](<https://attack.mitre.org/techniques/T1595>) or [Phishing for Information](<https://attack.mitre.org/techniques/T1598>). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](<https://attack.mitre.org/techniques/T1593/001>) or [Search Victim-Owned Websites](<https://attack.mitre.org/techniques/T1594>)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](<https://attack.mitre.org/techniques/T1593>) or [Search Open Technical

Databases](<https://attack.mitre.org/techniques/T1596>)), establishing operational resources (ex: [Develop Capabilities](<https://attack.mitre.org/techniques/T1587>) or [Obtain Capabilities](<https://attack.mitre.org/techniques/T1588>)), and/or initial access (ex: [Supply Chain Compromise](<https://attack.mitre.org/techniques/T1195>) or [External Remote Services](<https://attack.mitre.org/techniques/T1133>)).

# Country

**Name**

United States

**Name**

United States

# Sector

**Name**

Technologies

**Description**

Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

**Name**

Technologies

**Description**

Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.



# Domain-Name

## Value

pdsguam.biz

pdsguam.biz

# External References

- 
- <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>
- 
- <https://www.cisa.gov/news-events/analysis-reports/ar24-038a>
- 
- <https://otx.alienvault.com/pulse/65c3ec19a033c43353a4fab8>