Jun 10 2023

NETMANAGEIT

Intelligence Report

Volt Typhoon targets US critical infrastructure with living-off-the-land techniques

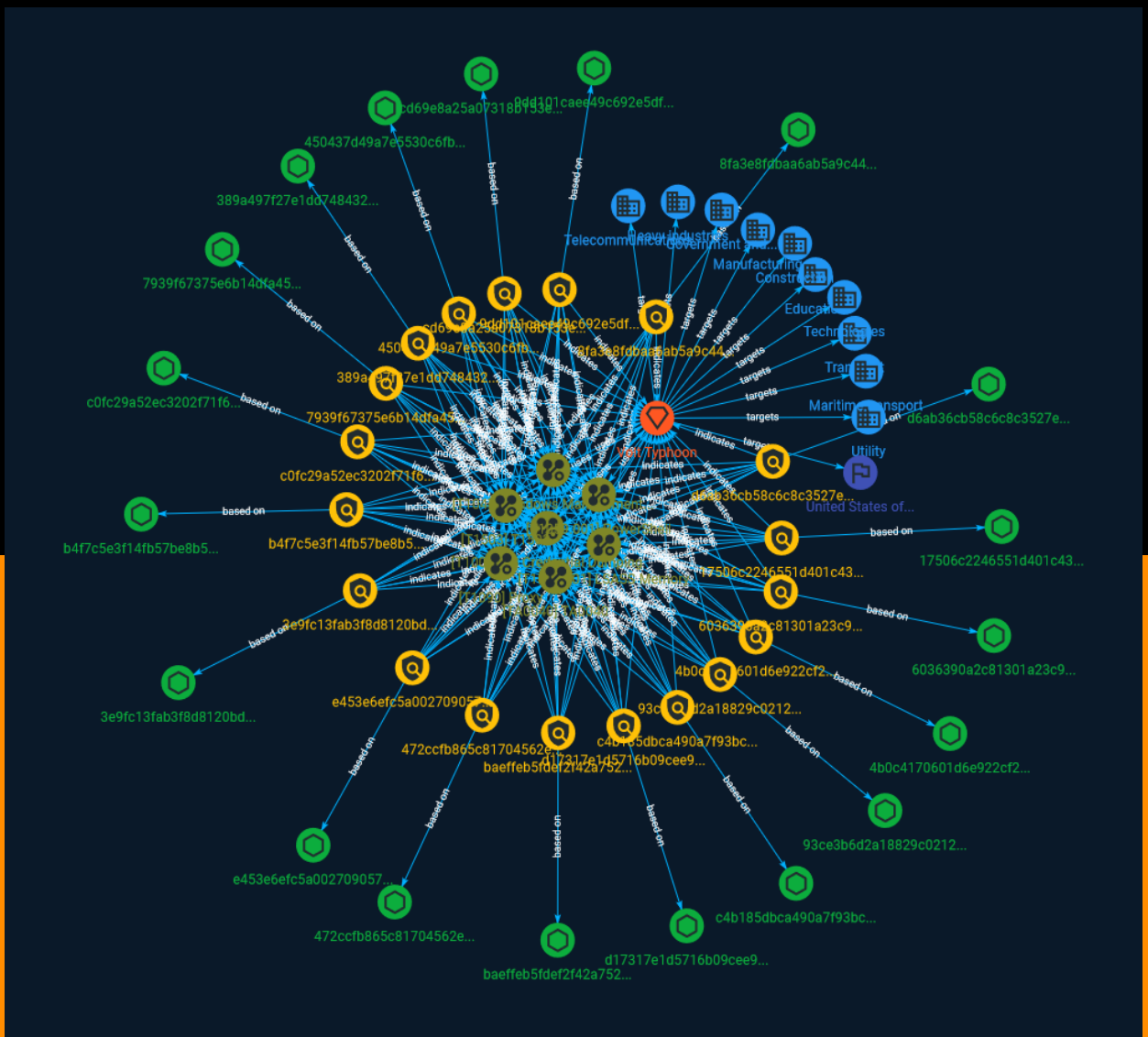

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Microsoft has uncovered stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the United States.

Confidence

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

15 / 100

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
Name
Windows Management Instrumentation
ID
T1047
Description
Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is an administration feature that provides a uniform

environment to access Windows system components. The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) (DCOM) and [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) (WinRM).(Citation: MSDN WMI) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: MSDN WMI)(Citation: FireEye WMI 2015) An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for Discovery as well as remote Execution of files as part of Lateral Movement. (Citation: FireEye WMI SANS 2015) (Citation: FireEye WMI 2015)

Name

PowerShell

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

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

LSASS Memory

ID

T1003.001

Description

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550). As well as in-memory

techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system. For example, on the target host use procdump: * `procdump -ma lsass.exe lsass_dump` Locally, mimikatz can be run using: * `sekurlsa::Minidump lsassdump.dmp` * `sekurlsa::logonPasswords` Built-in Windows tools such as comsvcs.dll can also be used: * `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full`(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector) Windows Security Support Provider (SSP) DLLs are loaded into LSASS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014) The following SSPs can be used to access credentials: * Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package. * Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. (Citation: TechNet Blogs Credential Protection) * Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later. * CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)

Name
TA0040
ID
TA0040
Name
T1503
ID
T1503

Sector

Name
Heavy industries
Description
Private entities working to transform raw materials into manufactured products (Chemicals, metal etc.).
Name
Education
Description
Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.
Name
Utility
Name
Manufacturing

Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.

Name
Transport

Description
All entities involved in the movement of people or goods from one place to another.

Name
Telecommunications

Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.

Name
Construction

Description
Private entities engaged in preparation of land and construction, alteration and repair of building, structures and other real estate properties.

Name
Maritime transport

Description
All entities transporting people or good by naval means, managing or exploiting naval structures (ports), naval constructors and traffic authorities.

Name
Government and administrations

Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Name
Technologies

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

Indicator

Name
472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d
Description
Volt Typhoon custom FRP executable
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d']
Name
450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267
Description
Volt Typhoon custom FRP executable
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267']

Name

4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349']

Name

b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74']

Name

8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2']

Name

d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295']

Name

7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5']

Name

17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4']

Name

e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95']

Name

cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984']

Name

93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066']

Name

c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d']

Name

d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af']

Name

baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c']

Name

389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61']

Name

6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff']

Name

3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642']

Name

9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a']

Name

c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b

Description

Volt Typhoon custom FRP executable

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b']

Intrusion-Set

Name
Volt Typhoon
Description
Imported from MISP tag

Country

Name
United States of America

StixFile

Value
3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642
c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d
9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a
17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4
6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff
b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74
c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b
cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984
389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61
4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349
7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5
d17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295
d6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af

e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95

baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c

472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d

8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2

450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267

93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066

External References

- https://otx.alienvault.com/pulse/646f7b3924bb523f5fe3f549
- https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/