Sep 11 2023

NETMANAGEIT

Intelligence Report

Analysis of Cuba ransomware gang activity and tooling

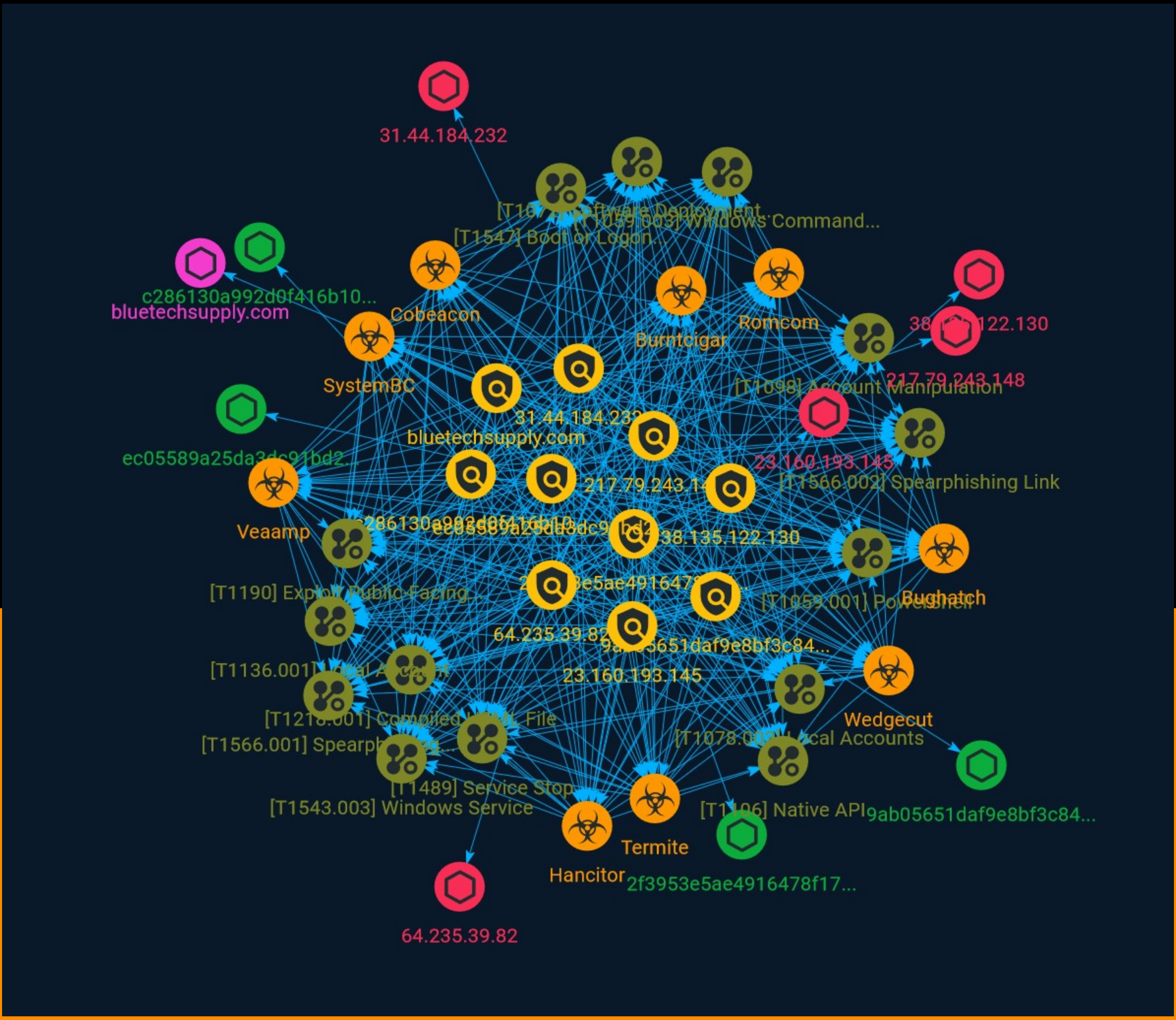

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report takes a close look at the history of the Cuba group, and their attack tactics, techniques and procedures.

Confidence

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

15 / 100

Indicator

Name
2f3953e5ae4916478f17b4dffc1cfed88a6ab2fbd2b3ab521ac20345c6091634
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2f3953e5ae4916478f17b4dffc1cfed88a6ab2fbd2b3ab521ac20345c6091634']
Name
ec05589a25da3dc91bd21a257b33f8c5bcc194835f445e227dad0485bf924239
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ec05589a25da3dc91bd21a257b33f8c5bcc194835f445e227dad0485bf924239']
Name

31.44.184.232

Description

CC=RU ASN=AS34665 Petersburg Internet Network ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '31.44.184.232']

Name

9ab05651daf9e8bf3c84b14613cd98e8479018bbcf3543521e94458012eba96e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ab05651daf9e8bf3c84b14613cd98e8479018bbcf3543521e94458012eba96e']

Name

c286130a992d0f416b103cd5a79b521a0a871146c0fda2912732341b77a463f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c286130a992d0f416b103cd5a79b521a0a871146c0fda2912732341b77a463f9']

Name

217.79.243.148

Description

ISP: HIVELOCITY, Inc. **OS:** Windows Server 2012 R2 (build 6.3.9600) -------------------------- Hostnames: - 217-79-243-148.static.hvvc.us -------------------------- Domains: - hvvc.us -------------------------- Services: **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Sun, 10 Sep 2023 01:46:07 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-25FFVSIPLS1 NetBIOS Domain Name: WIN-25FFVSIPLS1 NetBIOS Computer Name: WIN-25FFVSIPLS1 DNS Domain Name: WIN-25FFVSIPLS1 FQDN: WIN-25FFVSIPLS1 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '217.79.243.148']

Name

23.160.193.145

Description

CC=US ASN=AS397270 NETINF-TRANSIT-AS

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.160.193.145']

Name

bluetechsupply.com

Pattern Type

stix

Pattern

[domain-name:value = 'bluetechsupply.com']

Name

38.135.122.130

Description

ISP: FOXCLOUD LLP **OS:** None ------------------------- Hostnames: - h130-us122.fcsrv.net ------------------------- Domains: - fcsrv.net ------------------------- Services: **80:** ``` HTTP/1.1 404 Not Found Content-Length: 127 Content-Type: text/html;charset=UTF-8 ``` ------------------ **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: WINDOWS-10-PRO0 NetBIOS Domain Name: WINDOWS-10-PRO0 NetBIOS Computer Name: WINDOWS-10-PRO0 DNS Domain Name: windows-10-pro0 FQDN: windows-10-pro0 ``` ------------------

Pattern Type
stix

Pattern
[ipv4-addr:value = '38.135.122.130']

Name
64.235.39.82

Description
ISP: Las Vegas NV Datacenter **OS:** Windows (Build 10.0.19041) ------------------------- Hostnames: - lasvegas-nv-datacenter.serverpoint.com ------------------------- Domains: - serverpoint.com ------------------------- Services: **443:** ``` HTTP/1.1 404 Not Found Content-Length: 127 Content-Type: text/html;charset=UTF-8 ``` HEARTBLEED: 2023/01/18 08:43:46 64.235.39.82:443 - SAFE ------------------ **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ------------------ **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: 98r5Q3Mb8 NetBIOS Domain Name: 98r5Q3Mb8 NetBIOS Computer Name: 98r5Q3Mb8 DNS Domain Name: 98r5Q3Mb8 FQDN: 98r5Q3Mb8 ``` ------------------

Pattern Type
stix

Pattern
[ipv4-addr:value = '64.235.39.82']

Malware

Name
Cobeacon

Name
Wedgecut

Name
Veaamp

Name
Burntcigar

Name
Termite

Name
SystemBC

Name
Bughatch

Name
Romcom

Name
Hancitor
Description
[Hancitor](https://attack.mitre.org/software/S0499) is a downloader that has been used by [Pony](https://attack.mitre.org/software/S0453) and other information stealing malware. (Citation: Threatpost Hancitor)(Citation: FireEye Hancitor)

Attack-Pattern

Name
Compiled HTML File
ID
T1218.001
Description
Adversaries may abuse Compiled HTML files (.chm) to conceal malicious code. CHM files are commonly distributed as part of the Microsoft HTML Help system. CHM files are compressed compilations of various content such as HTML documents, images, and scripting/web related programming languages such VBA, JScript, Java, and ActiveX. (Citation: Microsoft HTML Help May 2018) CHM content is displayed using underlying components of the Internet Explorer browser (Citation: Microsoft HTML Help ActiveX) loaded by the HTML Help executable program (hh.exe). (Citation: Microsoft HTML Help Executable Program) A custom CHM file containing embedded payloads could be delivered to a victim then triggered by [User Execution](https://attack.mitre.org/techniques/T1204). CHM execution may also bypass application application control on older and/or unpatched systems that do not account for execution of binaries through hh.exe. (Citation: MsitPros CHM Aug 2017) (Citation: Microsoft CVE-2017-8625 Aug 2017)
Name
Software Deployment Tools
ID

T1072

Description

Adversaries may gain access to and use third-party software suites installed within an enterprise network, such as administration, monitoring, and deployment systems, to move laterally through the network. Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, HBSS, Altiris, etc.). Access to a third-party network-wide or enterprise-wide software system may enable an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to other systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints. The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the third-party system, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform it's intended purpose.

Name

Local Accounts

ID

T1078.003

Description

Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service. Local Accounts may also be abused to elevate privileges and harvest credentials through [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). Password reuse may allow the abuse of local accounts across a set of machines on a network for the purposes of Privilege Escalation and Lateral Movement.

Name

Local Account

ID

T1136.001

Description

Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service. With a sufficient level of access, the `net user /add` command can be used to create a local account. On macOS systems the `dscl -create` command can be used to create a local account. Local accounts may also be added to network devices, often via common [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `username`.(Citation: cisco_username_cmd) Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

Name

Account Manipulation

ID

T1098

Description

Adversaries may manipulate accounts to maintain access to victim systems. Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials. In order to create or manipulate accounts, the adversary must already have sufficient permissions on systems or the domain. However, account manipulation may also lead to privilege escalation where modifications grant access to additional roles, permissions, or higher-privileged [Valid Accounts](https://attack.mitre.org/techniques/T1078).

Name

Service Stop

ID

T1489

Description

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos Olympic Destroyer 2018)(Citation: Novetta Blockbuster) Adversaries may accomplish this by disabling individual services of high importance to an organization, such as `MSExchangeIS`, which will make Exchange content inaccessible (Citation: Novetta Blockbuster). In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct [Data Destruction](https://attack.mitre.org/techniques/T1485) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) on the data stores of services like Exchange and SQL Server.(Citation: SecureWorks WannaCry Analysis)

Name

Boot or Logon Autostart Execution

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation:

MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

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

Spearphishing Attachment

ID

T1566.001

Description

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Name

Windows Command Shell

ID

T1059.003

Description

Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows) Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems. Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.(Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

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

Spearphishing Link

ID

T1566.002

Description

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an "IDN homograph attack").(Citation: CISA IDN ST05-016) Adversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: Trend Micro Pawn Storm OAuth 2017) These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls. (Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

Name

Windows Service

ID

T1543.003

Description

Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions.(Citation: TechNet Services) Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry. Adversaries may install a new service or modify an existing service to execute at startup in order to persist on a system. Service configurations can be set or modified using system utilities (such as sc.exe), by directly modifying the Registry, or by interacting directly with the Windows API. Adversaries may also use services to install and execute malicious drivers. For example, after dropping a driver file (ex: `.sys`) to disk, the payload can be loaded and registered via [Native API](https://attack.mitre.org/techniques/T1106) functions such as `CreateServiceW()` (or manually via functions such as `ZwLoadDriver()` and `ZwSetValueKey()`), by creating the required service Registry values (i.e. [Modify Registry](https://attack.mitre.org/techniques/T1112)), or by using command-line utilities such as `PnPUtil.exe`.(Citation: Symantec W.32 Stuxnet Dossier)(Citation: Crowdstrike DriveSlayer February 2022)(Citation: Unit42 AcidBox June 2020) Adversaries may leverage these drivers as [Rootkit](https://attack.mitre.org/techniques/T1014)s to hide the presence of malicious activity on a system. Adversaries may also load a signed yet vulnerable driver onto a compromised machine (known as "Bring Your Own Vulnerable Driver" (BYOVD)) as part of [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges. Adversaries may also directly start services through [Service Execution](https://attack.mitre.org/techniques/T1569/002). To make detection analysis more challenging, malicious services may also incorporate [Masquerade Task or Service](https://attack.mitre.org/techniques/T1036/004) (ex: using a service and/or payload name related to a legitimate OS or benign software component).

Domain-Name

Value
bluetechsupply.com

StixFile

Value
c286130a992d0f416b103cd5a79b521a0a871146c0fda2912732341b77a463f9
2f3953e5ae4916478f17b4dffc1cfed88a6ab2fbd2b3ab521ac20345c6091634
ec05589a25da3dc91bd21a257b33f8c5bcc194835f445e227dad0485bf924239
9ab05651daf9e8bf3c84b14613cd98e8479018bbcf3543521e94458012eba96e

IPv4-Addr

Value
23.160.193.145
217.79.243.148
31.44.184.232
38.135.122.130
64.235.39.82

External References

- https://otx.alienvault.com/pulse/64ff8bf6100833b8c1573b83
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/09/11091834/Cuba-ransomware-IoCs.pdf
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/09/11095522/Cuba-ransomware-TTPs.pdf
- https://securelist.com/cuba-ransomware/110533/