Jun 27 2024

NETMANAGEIT

Intelligence Report

Chamelgang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware

7604e9ecedf298907e53...
8679c9e96394c39fa5ee...
china chopper
[T1112] T1112
[T1022] T1022
Cobalt Strike
cf2b73f77761f4441f9c...
49292dd838429bcf4aaf...
ransomware
conti
185.225.19.62
wiper
ChamelGang
icedid
[T1574.001] T1574.001
Manufacturing
9990388776daa57d2b06...
806761850d19f0cc9f41...
uses
based-on
indicates
targets
part-of

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In collaboration with Recorded Future, SentinelLabs has been tracking two distinct activity clusters targeting government and critical infrastructure sectors globally between 2021 and 2023.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name
T1112
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

T1574.001

ID

T1574.001

Description

Adversaries may execute their own malicious payloads by hijacking the search order used to load DLLs. Windows systems use a common method to look for required DLLs to load into a program. (Citation: Microsoft Dynamic Link Library Search Order)(Citation: FireEye Hijacking July 2010) Hijacking DLL loads may be for the purpose of establishing persistence as well as elevating privileges and/or evading restrictions on file execution. There are many ways an adversary can hijack DLL loads. Adversaries may plant trojan dynamic-link library files (DLLs) in a directory that will be searched before the location of a legitimate library that will be requested by a program, causing Windows to load their malicious library when it is called for by the victim program. Adversaries may also perform DLL preloading, also called binary planting attacks, (Citation: OWASP Binary Planting) by placing a malicious DLL with the same name as an ambiguously specified DLL in a location that Windows searches before the legitimate DLL. Often this location is the current working directory of the program.(Citation: FireEye fxsst June 2011) Remote DLL preloading attacks occur when a program sets its current directory to a remote location such as a Web share before loading a DLL. (Citation: Microsoft Security Advisory 2269637) Phantom DLL hijacking is a specific type of DLL search order hijacking where adversaries target references to non-existent DLL files.(Citation: Adversaries Hijack DLLs) They may be able to load their own malicious DLL by planting it with the correct name in the location of the missing module. Adversaries may also directly modify the search order via DLL redirection, which after being enabled (in the Registry and creation of a redirection file) may cause a program to load a different DLL.(Citation: Microsoft Dynamic-Link Library Redirection)(Citation: Microsoft Manifests)(Citation: FireEye DLL Search Order Hijacking) If a search order-vulnerable program is configured to run at a higher privilege level, then the adversary-controlled DLL that is loaded will also be executed at the higher level. In this case, the technique could be used for privilege escalation from user to administrator or SYSTEM or from administrator to SYSTEM, depending on the program. Programs that fall victim to path hijacking may appear to behave normally because malicious DLLs may be configured to also load the legitimate DLLs they were meant to replace.

Name

T1022

ID

T1022

Description

Data is encrypted before being exfiltrated in order to hide the information that is being exfiltrated from detection or to make the exfiltration less conspicuous upon inspection by a defender. The encryption is performed by a utility, programming library, or custom algorithm on the data itself and is considered separate from any encryption performed by the command and control or file transfer protocol. Common file archive formats that can encrypt files are RAR and zip. Other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048)

Sector

Name
Critical Infrastructure
Description
Private entities working to transform raw materials into manufactured products (Chemicals, metal etc.).
Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Government
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Indicator

Name	cf2b73f77761f4441f9c31512d58709f5d9d59eef6514857a5e37b8c4e956c3a
Description	ConventionEngine_Term_Users SHA256 of 09959be9b5f8ca21caa55577ce620034632a3f92
Pattern Type	stix
Pattern	[file:hashes.'SHA-256' = 'cf2b73f77761f4441f9c31512d58709f5d9d59eef6514857a5e37b8c4e956c3a']
Name	185.225.19.61
Description	**ISP:** MivoCloud SRL **OS:** - ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCehLTIJNCbue7D8DuOayN/BbrRJSJnelgpETy/T7aDpcqyDpT14FnVytp0RnU/EHBBhmvniFdUmeXEI+sKHaYvrK4/jXTBb3VHBUmILinQaJg/b6zgntGvmPKtNpDTwfGJaHKnDGOxwXWxRkWKi2s9Echod/yFt/XrgvrlNIw7nUF63uEMyS20NoosYkPG7N0mnctO

6qwGCCdRgnXoo0ed+CpWfP4vqh8wkmHxQNEmu4cgt0yhn0pMJdSN8PuPN0ZBeXSkWoTFEQ pVK5DS 795bdGSMlyHJ9EKGAx/iTHbfU5P2MsM5QcjxU42SOmtGjPN5cieekyHapKfPlDeoGBph Fingerprint: 95:85:9a:a8:18:98:d3:c8:ca:b8:d2:27:cd:db:57:2a Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ```

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.225.19.61']

Name

8679c9e96394c39fa5eeb277a7e28313ef502be5d8401c43fa9955820962add0

Description

stack_string SHA256 of dfab55758b195d1d30d89ba9175da3a49dc180be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8679c9e96394c39fa5eeb277a7e28313ef502be5d8401c43fa9955820962add0']

Name

806761850d19f0cc9f41618e74db471e85c494e952f900f827c1779f2d1c4d31

Description

SHA256 of 44759a6597bad3a287a7b82724a763208c599135

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '806761850d19f0cc9f41618e74db471e85c494e952f900f827c1779f2d1c4d31']

Name

49292dd838429bcf4aaf77ff6960156edaf1ec094ee4e6b9863c5d5fc9d32279

Description

SHA256 of 951e603af10ec366ef0f258bf8d912efedbb5a4b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'49292dd838429bcf4aaf77ff6960156edaf1ec094ee4e6b9863c5d5fc9d32279']

Name

9990388776daa57d2b06488f9e2209e35ef738fd0be1253be4c22a3ab7c3e1e2

Description

Win64:Malware-gen SHA256 of db99fc79a64873bef25998681392ac9be2c1c99c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'9990388776daa57d2b06488f9e2209e35ef738fd0be1253be4c22a3ab7c3e1e2']

Name

7604e9ecedf298907e537e50b9c74006640561b32265c3ebba38e587166f67ab

Description

ConventionEngine_Term_Users SHA256 of a79bc5e91761c98d99dc028401cd284c3b340474

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7604e9ecedf298907e537e50b9c74006640561b32265c3ebba38e587166f67ab']

Name

bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz

Pattern Type

stix

Pattern

[cryptocurrency-wallet:value = 'bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz']

Intrusion-Set

Name
ChamelGang

Malware

Name

conti

Description

[Conti](https://attack.mitre.org/software/S0575) is a Ransomware-as-a-Service (RaaS) that was first observed in December 2019. [Conti](https://attack.mitre.org/software/S0575) has been deployed via [TrickBot](https://attack.mitre.org/software/S0266) and used against major corporations and government agencies, particularly those in North America. As with other ransomware families, actors using [Conti](https://attack.mitre.org/software/S0575) steal sensitive files and information from compromised networks, and threaten to publish this data unless the ransom is paid.(Citation: Cybereason Conti Jan 2021)(Citation: CarbonBlack Conti July 2020)(Citation: Cybleinc Conti January 2020)

Name

wiper

Description

[Wiper](https://attack.mitre.org/software/S0041) is a family of destructive malware used in March 2013 during breaches of South Korean banks and media companies. (Citation: Dell Wiper)

Name

ransomware

Name

china chopper

Description

[China Chopper](https://attack.mitre.org/software/S0020) is a [Web Shell](https://attack.mitre.org/techniques/T1505/003) hosted on Web servers to provide access back into an enterprise network that does not rely on an infected system calling back to a remote command and control server.(Citation: Lee 2013) It has been used by several threat groups.(Citation: Dell TG-3390)(Citation: FireEye Periscope March 2018)(Citation: CISA AA21-200A APT40 July 2021)(Citation: Rapid7 HAFNIUM Mar 2021)

Name

Cobalt Strike

Description

[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

Name

icedid

Description

[IcedID](https://attack.mitre.org/software/S0483) is a modular banking malware designed to steal financial information that has been observed in the wild since at least 2017. [IcedID](https://attack.mitre.org/software/S0483) has been downloaded by [Emotet] (https://attack.mitre.org/software/S0367) in multiple campaigns.(Citation: IBM IcedID November 2017)(Citation: Juniper IcedID June 2020)

uses

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

indicates

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

targets

Name
Name
Name
Name
Name
Name
Name
Name

based-on

Name

Name

Name

Name

Name

part-of

Name

Description
Sector Heavy industries is a subsector of Manufacturing

Cryptocurrency-Wallet

Value
bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz

StixFile

Value
806761850d19f0cc9f41618e74db471e85c494e952f900f827c1779f2d1c4d31
8679c9e96394c39fa5eeb277a7e28313ef502be5d8401c43fa9955820962add0
9990388776daa57d2b06488f9e2209e35ef738fd0be1253be4c22a3ab7c3e1e2
49292dd838429bcf4aaf77ff6960156edaf1ec094ee4e6b9863c5d5fc9d32279
7604e9ecedf298907e537e50b9c74006640561b32265c3ebba38e587166f67ab
cf2b73f77761f4441f9c31512d58709f5d9d59eef6514857a5e37b8c4e956c3a

IPv4-Addr

Value
185.225.19.61

External References

- https://assets.sentinelone.com/sentinellabs/chamelgang-friends-en
- https://otx.alienvault.com/pulse/667c50c56fd52a7b4ecd11f2