Jun 10 2023

NETMANAGEIT

Intelligence Report

Core Werewolf against the defense industry and critical infrastructure

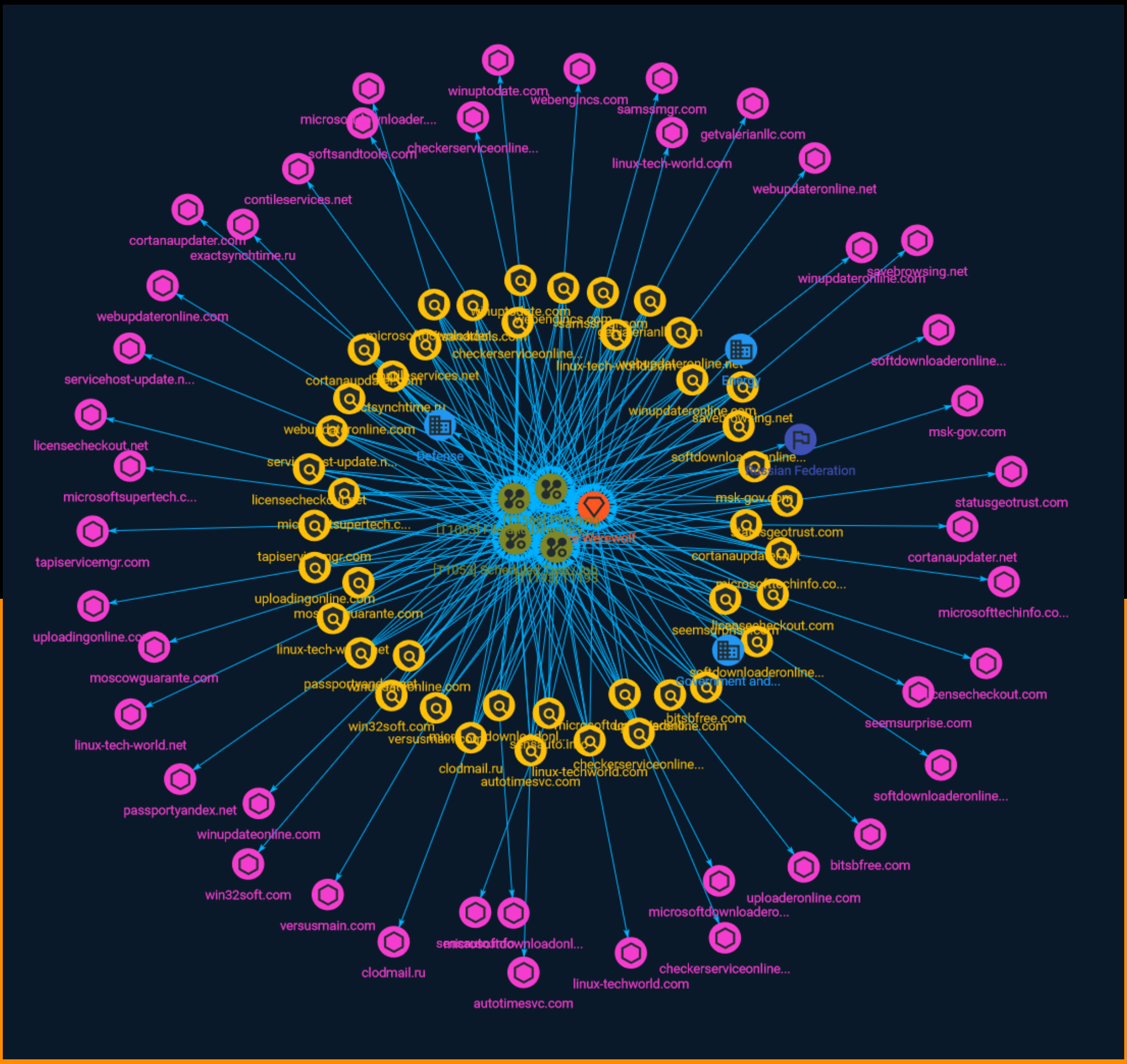

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Attack-Pattern 5
- Sector 8
- Indicator 9
- Intrusion-Set 24
- Country 25

Observables

- Domain-Name 26

External References

● External References 29

Overview

Description

The Core Werewolf group is one of the newest representatives of the part of cybercrime that is actively engaged in espionage in today's environment. Since at least 2021, it has launched attacks on Russian organizations associated with the military-industrial complex (DIC) and critical information infrastructure (CII)

Confidence

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

15 / 100

Attack-Pattern

Name
Scheduled Task/Job
ID
T1053
Description
Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)
Name
Phishing
ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1193

ID

T1193

Name

File and Directory Discovery

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Sector

Name

Energy

Description

Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.

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

Defense

Description

Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

Indicator

Name
softdownloaderonline.net
Pattern Type
stix
Pattern
[domain-name:value = 'softdownloaderonline.net']
Name
win32soft.com
Pattern Type
stix
Pattern
[domain-name:value = 'win32soft.com']
Name
checkerserviceonline.com

Pattern Type
stix
Pattern
[domain-name:value = 'checkerserviceonline.com']
Name
licensecheckout.com
Pattern Type
stix
Pattern
[domain-name:value = 'licensecheckout.com']
Name
winupdateonline.com
Pattern Type
stix
Pattern
[domain-name:value = 'winupdateonline.com']
Name
linux-tech-world.com

Pattern Type

stix

Pattern

[domain-name:value = 'linux-tech-world.com']

Name

autotimesvc.com

Pattern Type

stix

Pattern

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

Name

exactsynchtime.ru

Pattern Type

stix

Pattern

[domain-name:value = 'exactsynchtime.ru']

Name

microsofttechinfo.com

Pattern Type

stix

Pattern

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

Name

microsoftdownloadonline.com

Pattern Type

stix

Pattern

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

Name

softsandtools.com

Pattern Type

stix

Pattern

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

Name

softdownloaderonline.com

Pattern Type

stix

Pattern

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

Name

moscowguarante.com

Pattern Type

stix

Pattern

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

Name

winupdateronline.com

Pattern Type

stix

Pattern

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

Name

microsoftdownloaderonline.com

Pattern Type
stix
Pattern
[domain-name:value = 'microsoftdownloaderonline.com']
Name
contileservices.net
Pattern Type
stix
Pattern
[domain-name:value = 'contileservices.net']
Name
seemsurprise.com
Pattern Type
stix
Pattern
[domain-name:value = 'seemsurprise.com']
Name
linux-tech-world.net

Pattern Type

stix

Pattern

[domain-name:value = 'linux-tech-world.net']

Name

winuptodate.com

Pattern Type

stix

Pattern

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

Name

uploaderonline.com

Pattern Type

stix

Pattern

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

Name

servicehost-update.net

Pattern Type

stix

Pattern

[domain-name:value = 'servicehost-update.net']

Name

savebrowsing.net

Pattern Type

stix

Pattern

[domain-name:value = 'savebrowsing.net']

Name

linux-techworld.com

Pattern Type

stix

Pattern

[domain-name:value = 'linux-techworld.com']

Name

cortanaupdater.com

Pattern Type

stix

Pattern

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

Name

bitsbfree.com

Pattern Type

stix

Pattern

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

Name

microsoftsupertech.com

Pattern Type

stix

Pattern

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

Name

getvalerianllc.com

Pattern Type

stix

Pattern

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

Name

clodmail.ru

Pattern Type

stix

Pattern

[domain-name:value = 'clodmail.ru']

Name

webupdateronline.com

Pattern Type

stix

Pattern

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

Name

cortanaupdater.net

Pattern Type
stix

Pattern
[domain-name:value = 'cortanaupdater.net']

Name
passportyandex.net

Pattern Type
stix

Pattern
[domain-name:value = 'passportyandex.net']

Name
samssmgr.com

Pattern Type
stix

Pattern
[domain-name:value = 'samssmgr.com']

Name
checkerserviceonline.net

Pattern Type

stix

Pattern

[domain-name:value = 'checkerserviceonline.net']

Name

tapiservicemgr.com

Pattern Type

stix

Pattern

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

Name

webupdateronline.net

Pattern Type

stix

Pattern

[domain-name:value = 'webupdateronline.net']

Name

versusmain.com

Pattern Type

stix

Pattern

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

Name

microsoftdownloader.com

Pattern Type

stix

Pattern

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

Name

statusgeotrust.com

Pattern Type

stix

Pattern

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

Name

uploadingonline.com

Pattern Type
stix
Pattern
[domain-name:value = 'uploadingonline.com']
Name
webengincs.com
Pattern Type
stix
Pattern
[domain-name:value = 'webengincs.com']
Name
sensauto.info
Pattern Type
stix
Pattern
[domain-name:value = 'sensauto.info']
Name
licensecheckout.net

Pattern Type
stix

Pattern
[domain-name:value = 'licensecheckout.net']

Name
msk-gov.com

Pattern Type
stix

Pattern
[domain-name:value = 'msk-gov.com']

Intrusion-Set

Name
Core Werewolf

Country

Name
Russian Federation

Domain-Name

Value
msk-gov.com
softsandtools.com
linux-techworld.com
versusmain.com
softdownloaderonline.net
tapiservicemgr.com
win32soft.com
bitsbfree.com
cortanaupdater.net
linux-tech-world.net
samssmgr.com
webengincs.com
contileservices.net

licensecheckout.net
sensauto.info
exactsynchtime.ru
webupdateronline.net
uploadingonline.com
winupdateronline.com
getvalerianllc.com
webupdateronline.com
winuptodate.com
softdownloaderonline.com
winupdateonline.com
clodmail.ru
uploaderonline.com
seemsurprise.com
autotimesvc.com
licensecheckout.com
checkerserviceonline.net
microsoftdownloader.com

moscowguarante.com
servicehost-update.net
microsoftdownloaderonline.com
cortanaupdater.com
savebrowsing.net
checkerserviceonline.com
linux-tech-world.com
microsoftsupertech.com
microsofttechinfo.com
statusgeotrust.com
microsoftdownloadonline.com
passportyandex.net

External References

- https://bi.zone/expertise/blog/core-werewolf-protiv-opk-i-kriticheskoy-infrastruktury/
- https://otx.alienvault.com/pulse/648347434c397b4817e63bf9