Dec 12 2023

NETMANAGEIT

Intelligence Report

Operation Blacksmith: Lazarus targets organizations worldwide using novel Telegram-based malware written in DLang

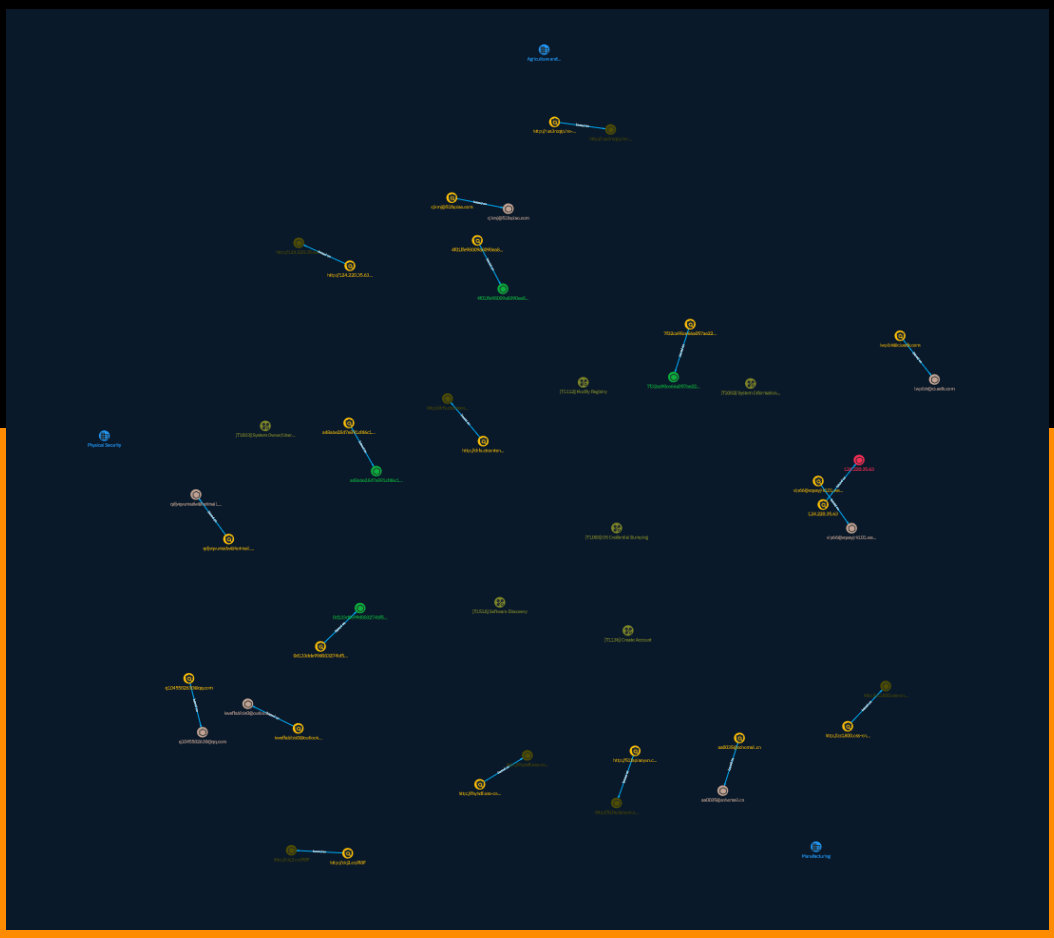

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Cisco Talos recently discovered a new campaign conducted by the Lazarus Group. This campaign has been called “Operation Blacksmith,” and they are employing at least three new DLang-based malware families, two of which are remote access trojans (RATs), where one of these uses Telegram bots and channels as a medium of command and control (C2) communications.

Confidence

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

15 / 100

Content

N/A

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
Software Discovery
ID
T1518
Description
Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information

from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

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

Create Account

ID

T1136

Description

Adversaries may create an account to maintain access to victim systems. With a sufficient level of access, creating such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system. Accounts may be created on the local system or within a domain or cloud tenant. In cloud environments, adversaries may create accounts that only have access to specific services, which can reduce the chance of detection.

Name

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the

device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Sector

Name
Agriculture and agribusiness
Description
Private entities specialized in the growth, culture, transport and transformation of plants or livestock for food.
Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Physical Security

Indicator

Name
vip66@xqxayjrk101.wecom.work
Pattern Type
stix
Pattern
[email-addr:value = 'vip66@xqxayjrk101.wecom.work']
Name
http://drfs.ctcontents.com/file/40788929/860577489/
Pattern Type
stix
Pattern
[url:value = 'http://drfs.ctcontents.com/file/40788929/860577489/']
Name
http://fhyhdf.oss-cn-hangzhou.aliyuncs.com/%E7%99%BC%E7%A5%A8.zip

Pattern Type

stix

Pattern

[url:value = 'http://fhyhdf.oss-cn-hangzhou.aliyuncs.com/%E7%99%BC%E7%A5%A8.zip']

Name

http://51fapiaoyun.com/%E5%8F%91-%E7%A5%A8.rar

Pattern Type

stix

Pattern

[url:value = 'http://51fapiaoyun.com/%E5%8F%91-%E7%A5%A8.rar']

Name

kweffabibis0@outlook.com

Pattern Type

stix

Pattern

[email-addr:value = 'kweffabibis0@outlook.com']

Name

4f01ffe98009a8090ea8a086d21c62c24219b21938ea3ec7da8072f8c4dcc7a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4f01ffe98009a8090ea8a086d21c62c24219b21938ea3ec7da8072f8c4dcc7a6']

Name

124.220.35.63

Description

ISP: Shenzhen Tencent Computer Systems Company Limited **OS:** Windows (build 6.3.9600) ---------- Hostnames: ---------- Domains: ---------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: 10_0_4_13 NetBIOS Domain Name: 10_0_4_13 NetBIOS Computer Name: 10_0_4_13 DNS Domain Name: 10_0_4_13 FQDN: 10_0_4_13 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '124.220.35.63']

Name

q1045582630@qq.com

Pattern Type

stix

Pattern

[email-addr:value = 'q1045582630@qq.com']

Name

http://124.220.35.63/laoxiang.exe

Pattern Type

stix

Pattern

[url:value = 'http://124.220.35.63/laoxiang.exe']

Name

http://ckj2.cn/R8F

Pattern Type

stix

Pattern

[url:value = 'http://ckj2.cn/R8F']

Name

a48abe2847e891cfd6c18c7cdaaa8e983051bc2f7a0bd9ef5c515a72954e1715

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a48abe2847e891cfd6c18c7cdaaa8e983051bc2f7a0bd9ef5c515a72954e1715']

Name

aa0035@zohomail.cn

Pattern Type

stix

Pattern

[email-addr:value = 'aa0035@zohomail.cn']

Name

0d133dde99d883274bf5644bd9e59af3c54c2b3c65f3d1bc762f2d3725f80582

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0d133dde99d883274bf5644bd9e59af3c54c2b3c65f3d1bc762f2d3725f80582']

Name

7f32ca98ce66a057ae226ec78638db95feebc59295d3afffdbf407df12b5bc79

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7f32ca98ce66a057ae226ec78638db95feebc59295d3afffdbf407df12b5bc79']

Name

http://zc1800.oss-cn-shenzhen.aliyuncs.com/piao

Pattern Type

stix

Pattern

[url:value = 'http://zc1800.oss-cn-shenzhen.aliyuncs.com/piao']

Name

cjkmj@51fapiao.com

Pattern Type

stix

Pattern

[email-addr:value = 'cjkmj@51fapiao.com']

Name

lwplbh@cluedk.com

Pattern Type

stix

Pattern

[email-addr:value = 'lwplbh@cluedk.com']

Name

qdjvqvumsdw@hotmail.com

Pattern Type

stix

Pattern

[email-addr:value = 'qdjvqvumsdw@hotmail.com']

Name

http://rus3rcqtp.hn-bkt.clouddn.com/26866498.zip

Pattern Type

stix

Pattern

[url:value = 'http://rus3rcqtp.hn-bkt.clouddn.com/26866498.zip']

Email-Addr

Value
vip66@xqxayjrk101.wecom.work
kweffabibis0@outlook.com
cjkmj@51fapiao.com
aa0035@zohomail.cn
qdjvqvumsdw@hotmail.com
lwplbh@cluedk.com
q1045582630@qq.com

StixFile

Value
a48abe2847e891cfd6c18c7cdaaa8e983051bc2f7a0bd9ef5c515a72954e1715
4f01ffe98009a8090ea8a086d21c62c24219b21938ea3ec7da8072f8c4dcc7a6
7f32ca98ce66a057ae226ec78638db95feebc59295d3afffdbf407df12b5bc79
0d133dde99d883274bf5644bd9e59af3c54c2b3c65f3d1bc762f2d3725f80582

IPv4-Addr

Value
124.220.35.63

Url

Value
http://51fapiaoyun.com/%E5%8F%91-%E7%A5%A8.rar
http://drfs.ctcontents.com/file/40788929/860577489/
http://zc1800.oss-cn-shenzhen.aliyuncs.com/piao
http://ckj2.cn/R8F
http://rus3rcqtp.hn-bkt.clouddn.com/26866498.zip
http://fhyhdf.oss-cn-hangzhou.aliyuncs.com/%E7%99%BC%E7%A5%A8.zip
http://124.220.35.63/laoxiang.exe

External References

- https://otx.alienvault.com/pulse/6578766e9d1a1cf4d6ee8aff
- https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/