Sep 20 2023

NETMANAGEIT

Intelligence Report

Earth Lusca Employs New Linux Backdoor, Uses Cobalt Strike for Lateral Movement

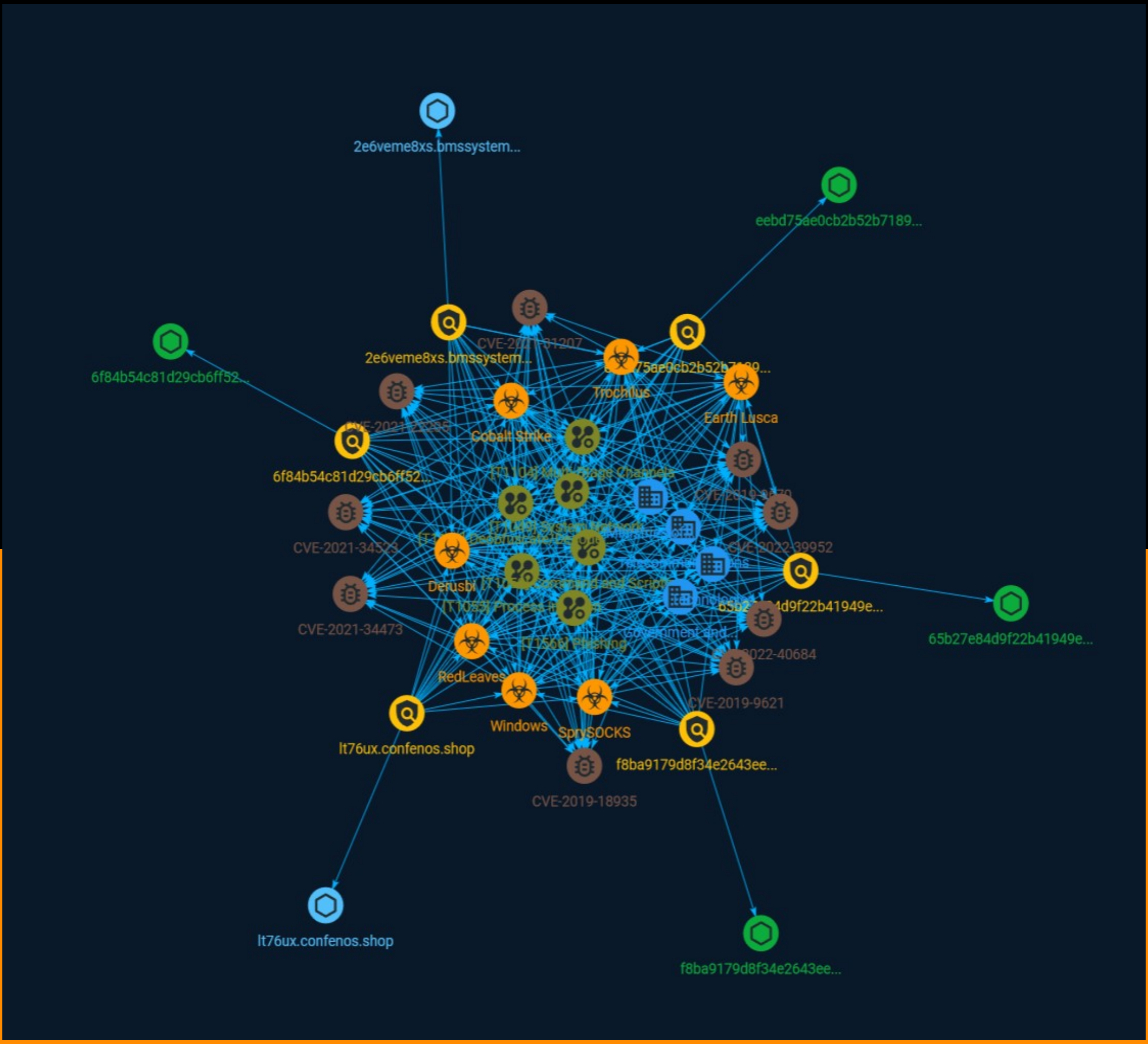

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Earth Lusca remained active during the first half of 2023, with its attacks focusing primarily on countries in Southeast Asia, Central Asia, and the Balkans (with a few scattered attacks on Latin American and African countries). The group's main targets are government departments that are involved in foreign affairs, technology, and telecommunications.

Confidence

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

15 / 100

Attack-Pattern

Name
Process Injection
ID
T1055
Description
Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.
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

Multi-Stage Channels

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

Sector

Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.
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
Ministries of foreign affairs
Description
Governmental entities in charge of the diplomatic action of the State.
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
eebd75ae0cb2b52b71890f84e92405ac30407c7a3fe37334c272fd2ab03dff58
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'eebd75ae0cb2b52b71890f84e92405ac30407c7a3fe37334c272fd2ab03dff58']
Name
f8ba9179d8f34e2643ee4f8bc51c8af046e3762508a005a2d961154f639b2912
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f8ba9179d8f34e2643ee4f8bc51c8af046e3762508a005a2d961154f639b2912']
Name

6f84b54c81d29cb6ff52ce66426b180ad0a3b907e2ef1117a30e95f2dc9959fc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f84b54c81d29cb6ff52ce66426b180ad0a3b907e2ef1117a30e95f2dc9959fc']

Name

65b27e84d9f22b41949e42e8c0b1e4b88c75211cbf94d5fd66edc4ebe21b7359

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '65b27e84d9f22b41949e42e8c0b1e4b88c75211cbf94d5fd66edc4ebe21b7359']

Name

lt76ux.confenos.shop

Pattern Type

stix

Pattern

[hostname:value = 'lt76ux.confenos.shop']

Name
2e6veme8xs.bmssystemg188.us
Pattern Type
stix
Pattern
[hostname:value = '2e6veme8xs.bmssystemg188.us']

Malware

Name

RedLeaves

Description

[RedLeaves](https://attack.mitre.org/software/S0153) is a malware family used by [menuPass](https://attack.mitre.org/groups/G0045). The code overlaps with [PlugX](https://attack.mitre.org/software/S0013) and may be based upon the open source tool Trochilus. (Citation: PWC Cloud Hopper Technical Annex April 2017) (Citation: FireEye APT10 April 2017)

Name

Trochilus

Name

SprySOCKS

Name

Derusbi

Description

[Derusbi](https://attack.mitre.org/software/S0021) is malware used by multiple Chinese APT groups.(Citation: Novetta-Axiom)(Citation: ThreatConnect Anthem) Both Windows and Linux variants have been observed.(Citation: Fidelis Turbo)

Name
Earth Lusca

Name
Windows

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)

Vulnerability

Name
CVE-2022-40684

Name
CVE-2021-34523

Name
CVE-2019-9670

Name
CVE-2019-18935

Name
CVE-2021-22205

Name
CVE-2022-39952

Name
CVE-2021-34473

Name
CVE-2021-31207

Name
CVE-2019-9621

StixFile

Value
65b27e84d9f22b41949e42e8c0b1e4b88c75211cbf94d5fd66edc4ebe21b7359
6f84b54c81d29cb6ff52ce66426b180ad0a3b907e2ef1117a30e95f2dc9959fc
eebd75ae0cb2b52b71890f84e92405ac30407c7a3fe37334c272fd2ab03dff58
f8ba9179d8f34e2643ee4f8bc51c8af046e3762508a005a2d961154f639b2912

Hostname

Value
2e6veme8xs.bmssystemg188.us
lt76ux.confenos.shop

External References

- https://otx.alienvault.com/pulse/6509cd6cb1f6826dace407d7
- https://www.trendmicro.com/en_us/research/23/i/earth-lusca-employs-new-linux-backdoor.html