Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

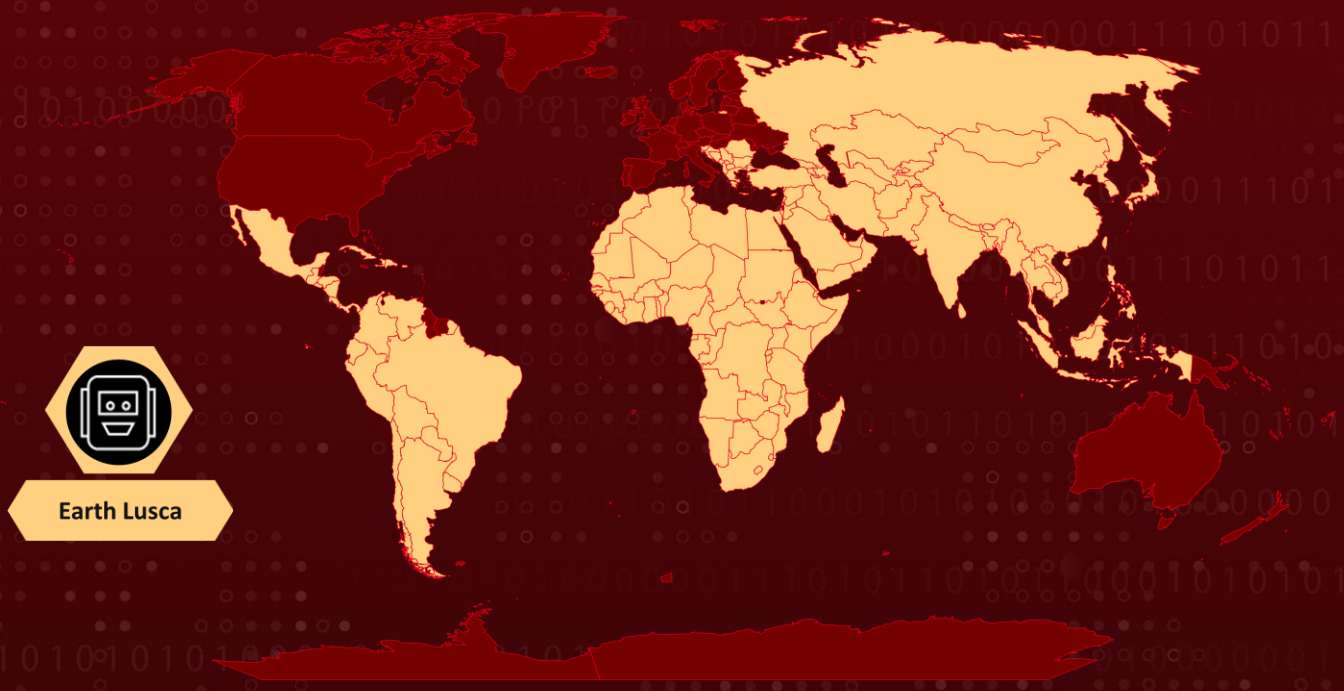
Earth Lusca's Sneaky Moves Unleashes New Linux Backdoor

Date of Publication	Admiralty code	TA Number
September 20, 2023	A1	TA2023379

Summary

First Appearance: April 2019
Actor Name: Earth Lusca (aka Bronze University, Charcoal Typhoon, Red Scylla)
Target Industries: Casinos And Gambling, Technology, Education, Government, Media, Telecommunications, Foreign Affairs, Human Rights, Political Organizations and Cryptocurrency Trading Platforms
Target Region: Asia, the Balkans, and a few scattered regions in Latin American and African countries
Malware: SprySOCKS Backdoor

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2022-40684	Fortinet Multiple Products Authentication Bypass Vulnerability	Fortinet Multiple Products	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2022-39952	Fortinet FortiNAC Remote Code Execution Vulnerability	FortiNAC versions 9.4.0-8.3.7	✗	✗	✓
CVE-2021-22205	GitLab Community and Enterprise Editions Remote Code Execution Vulnerability	GitLab Community and Enterprise Editions	✗	✓	✓
CVE-2019-18935	Progress Telerik UI for ASP.NET AJAX Deserialization of Untrusted Data Vulnerability	Progess Telerik UI for ASP.NET AJAX	✗	✓	✓
CVE-2019-9670	Synacor Zimbra Collaboration (ZCS) Improper Restriction of XML External Entity Reference	Synacor Zimbra Collaboration (ZCS)	✗	✓	✓
CVE-2019-9621	Zimbra Server-Side Request Forgery Vulnerability	Zimbra Collaboration	✗	✗	✓
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	Microsoft Exchange Server	✗	✓	✓

Actor Details

#1

Earth Lusca, a threat actor with known affiliations to China and aliases such as Bronze University, Charcoal Typhoon, and Red Scylla, has been operational since April 2019. Notably, Earth Lusca has continued its activities throughout the first half of 2023, with a primary focus on targeting government departments engaged in foreign affairs, technology, and telecommunications.

#2

Earth Lusca's modus operandi involves the utilization of a previously undisclosed Linux backdoor named SprySOCKS. The infiltration campaigns orchestrated by Earth Lusca commence with the exploitation of known security vulnerabilities in the publicly accessible servers of their victims.

#3

Furthermore, they exhibit a proactive approach by exploiting n-day vulnerabilities in server-based systems, which include Fortinet (CVE-2022-39952 and CVE-2022-40684), GitLab (CVE-2021-22205), Microsoft Exchange Server (ProxyShell), Progress Telerik UI (CVE-2019-18935), and Zimbra (CVE-2019-9621 and CVE-2019-9670) servers. This exploitation results in the deployment of web shells and the delivery of Cobalt Strike for lateral movement within the compromised infrastructure.

#4

Earth Lusca's ultimate objectives encompass the exfiltration of sensitive documents and email account credentials. To facilitate prolonged espionage activities, they employ advanced backdoors like ShadowPad and a Linux variant of Winnti. The SprySOCKS backdoor is loaded through a variant of an ELF injector component referred to as 'mandibule.'

#5

SprySOCKS functionality includes the collection of system information, the initiation of an interactive shell, the creation and termination of SOCKS proxies, as well as the execution of various file and directory operations. It is worth noting that the implementation of the interactive shell in SprySOCKS appears to draw inspiration from the Linux version of a fully-featured backdoor known as Derusbi (also recognized as Photo), which has been associated with multiple Chinese threat activity clusters since at least 2008.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Earth Lusca (aka Bronze University, Charcoal Typhoon, Red Scylla)	China **MOTIVE** Information theft and espionage, Financial gain	Asia, the Balkans, and a few scattered regions in Latin	Casinos And Gambling, Technology, Education, Government, Media, Telecommunications, Foreign Affairs, Human Rights, Political Organizations and Cryptocurrency Trading Platforms

Recommendations

Patch and Update Vulnerable Software: Regularly update and patch all software and systems, particularly addressing known vulnerabilities. Ensure your software remains up to date by regularly checking for and applying the latest security updates and patches from the vendor patches can help prevent exploitation by threat actors like Earth Lusca.

Assess Third-Party Security: Evaluate the cybersecurity practices of third-party vendors and contractors who have access to your network or data. Ensure they adhere to robust security standards.

Enhance Network Monitoring: Invest in robust network monitoring and intrusion detection systems to quickly detect and respond to suspicious activities. Early detection can mitigate the damage caused by potential breaches.

Harden Server Configurations: Apply server hardening techniques to reduce the attack surface by disabling unnecessary services, closing unused ports, and following industry best practices for server security.

Implement DNS Filtering: Employ DNS filtering services to block access to known malicious domains and prevent malware communication with command-and-control servers.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0005 Defense Evasion	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0009** Collection
T1190 Exploit Public-Facing Application	**T1595.002** Vulnerability Scanning	**T1584.004** Server	**T1543** Create or Modify System Process
T1055 Process Injection	**T1570** Lateral Tool Transfer	**T1112** Modify Registry	**T1588.001** Malware
T1007 System Service Discovery	**T1560** Archive Collected Data		

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	65b27e84d9f22b41949e42e8c0b1e4b88c75211cbf94d5fd66edc4ebe21b7359, 6f84b54c81d29cb6ff52ce66426b180ad0a3b907e2ef1117a30e95f2dc9959fc, f8ba9179d8f34e2643ee4f8bc51c8af046e3762508a005a2d961154f639b2912, eebd75ae0cb2b52b71890f84e92405ac30407c7a3fe37334c272fd2ab03dff58
IPv4	207.148.75[.]122
Domains	lt76ux.confenos[.]shop, 2e6veme8xs.bmssystemg188[.]us

Patch Link

https://fortiguard.com/psirt/FG-IR-22-377

https://fortiguard.com/psirt/FG-IR-22-300

https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json

https://www.telerik.com/support/kb/aspnet-ajax/details/allows-javascriptserializer-deserialization

https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

https://wiki.zimbra.com/wiki/Security_Center

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

References

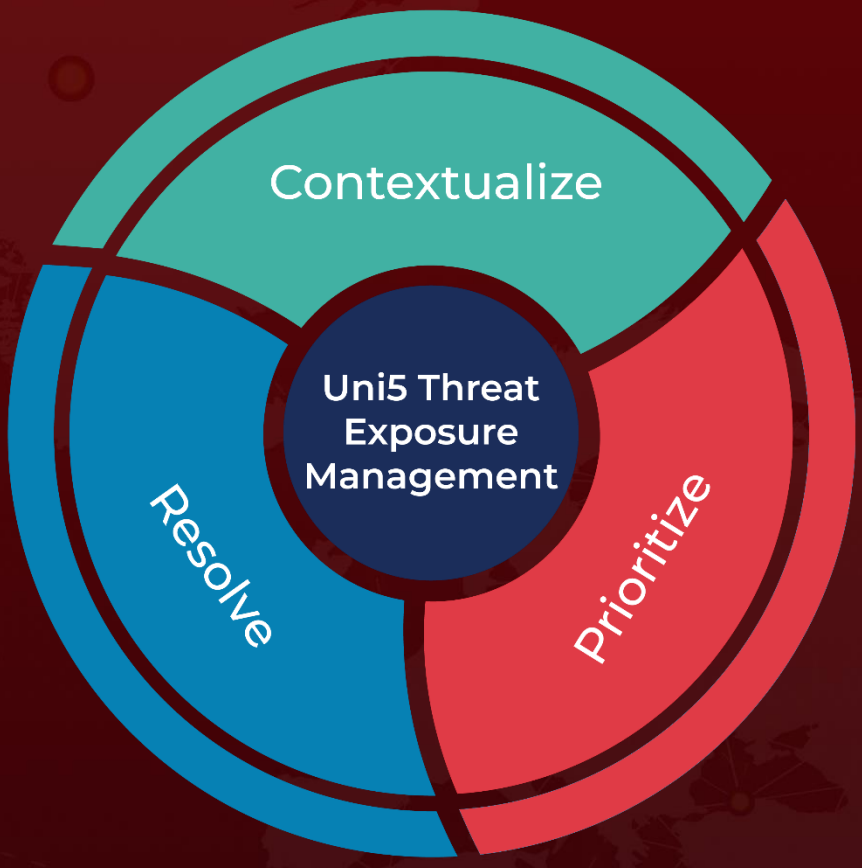
https://www.trendmicro.com/en_us/research/23/i/earth-lusca-employs-new-linux-backdoor.html

https://attack.mitre.org/groups/G1006/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 20, 2023 . 9:00 PM

More at www.hivepro.com