Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

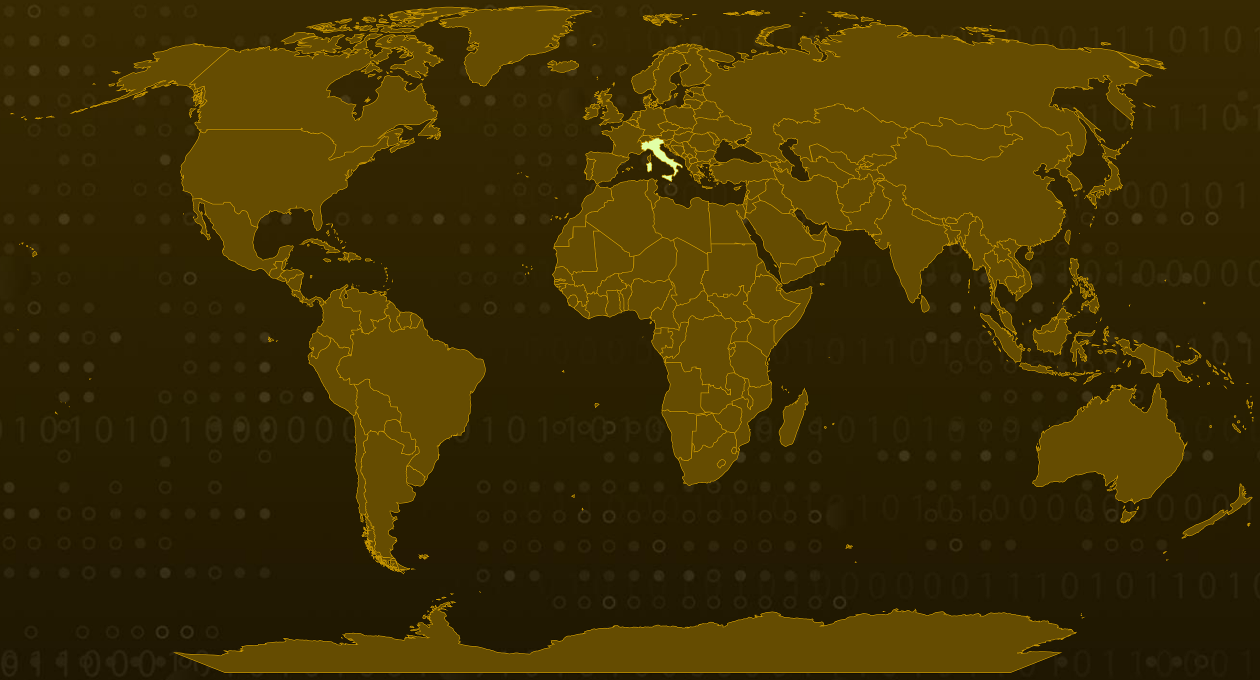
SambaSpy RAT a New Breed of Malware Targeting Italy

Date of Publication	Admiralty Code	TA Number
September 20, 2024	A1	TA2024364

Summary

First Seen: May 2024
Malware: SambaSpy RAT
Targeted Country: Italy
Attack: SambaSpy is a remote access Trojan (RAT) discovered in May 2024, specifically crafted to target Italian-speaking users through an advanced phishing campaign. This malware is notable for its highly targeted infection techniques, using language and system checks to ensure it only infects victims with Italian configurations.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 SambaSpy is a remote access Trojan (RAT) first discovered in May 2024, specifically designed to target Italian users. What distinguishes this campaign is its precision, using multiple infection checks to ensure it only affects Italian-speaking victims. However, there are signs that the attackers may have extended their operations to Spain, Brazil, and potentially other regions.

#2 The attackers communicated in Brazilian Portuguese, and while Italian users were the primary focus, links to Brazil suggest a wider agenda. Italian users were typically targeted by phishing emails from a German email address, written fluently in Italian and made to resemble legitimate communications from an Italian real estate company.

#3 Victims were redirected to FattureInCloud, a legitimate Italian cloud service for managing digital invoices. At the same time, some were sent to a malicious server that checked whether their operating system was set to Italian and if their browser was Edge, Chrome, or Firefox. If the system passed these checks, victims were directed to a Microsoft OneDrive-hosted PDF containing another link, leading to the download of a malicious JAR file from MediaFire, which is either a dropper or a downloader.

#4 This JAR file deliveres the final payload—the SambaSpy RAT. SambaSpy is a versatile tool with a range of features for spying and data theft. Written in Java and obfuscated using Zelix KlassMaster to evade detection, it enables full-scale surveillance, including screenshots, webcam control, keylogging, clipboard manipulation, system control, and credential theft.

Recommendations

Enhance Email Security with Anti-Phishing Tools: Use tools that detect and block phishing attempts, especially those impersonating legitimate entities. Regularly educate users on recognizing phishing emails that mimic legitimate organizations, especially in native languages.

Enhance Network Security and Segmentation: Separate critical network infrastructure to limit lateral movement if SambaSpy RAT or other malware gains access to a system. Continuously monitor network traffic for unusual patterns, such as connections to external servers like MediaFire or other malicious IP addresses.

Harden Systems Access Controls and Credential Security: Use credential guard technologies and regularly monitor for suspicious credential access or dumping activities. Rotate administrative credentials regularly and ensure that credentials are not reused across different systems or vendors.

Implement Robust Endpoint Protection: Use solutions that detect and block JAR file droppers, especially those obfuscated with Zelix KlassMaster. Employ EDR solutions to detect unusual behavior, such as JAR file executions or suspicious payload deliveries.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0011 Command and Control	**TA0010** Exfiltration	**T1056** Input Capture	**T1082** System Information Discovery
T1566 Phishing	**T1566.002** Spearphishing Link	**T1204** User Execution	**T1204.002** Malicious File
T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1036** Masquerading	**T1036.005** Match Legitimate Name or Location
T1056.001 Keylogging	**T1003** OS Credential Dumping	**T1046** Network Service Discovery	**T1113** Screen Capture
T1115 Clipboard Data	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1041** Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	e6be6bc2f8e27631a7bfd2e3f06494aa, 1ec21bd711b491ad47d5c2ef71ff1a10, d153006e00884edf7d48b9fe05d83cb4, 0f3b46d496bbf47e8a2485f794132b48
SHA1	c7fd7a4d33469f33f1986f20b8d638e77e4d3768, 73ce7c32ab8ce157b968eb49c4655f9d98926b71, ba17cba48578e8febf2591f9157b37652108f89a, 28911b5edd5235db1119acd2e09349320d665b88
SHA256	43f86b6d3300050f8cc0fa83948fbc92fc69af546f1f215313bad2e2a040c0fa, d3effd483815a7de1e1288ab6f4fb673b44a129386ef461466472e22140d47f8, 49bbfac69ca7633414172ec07e996d0dabd3f7811f134eecafe89acb8d55b93a, 9948b75391069f635189c5c5e24c7fafd88490901b204bcd4075f72ece5ec265
Domain	officediraccoltaanabelacosta[.]net, belliniepecuniaimmobili[.]com, immobilibelliniepecunia[.]xyz, immobilibelliniepecunia[.]online, immobilibelliniepecunia[.]site, bpecuniaimmobili[.]online, bpecuniaimmobili[.]info, belliniepecuniaimmobilisrl[.]shop, belliniepecuniaimmobilisrl[.]online, belliniepecuniaimmobilisrl[.]xyz, belliniepecuniaimmobili.com[.]br, bpecuniaimmobili[.]xyz, immobilibelliniepecunia[.]shop, immobilibelliniepecunia[.]me, immobiliarebelliniepecunia[.]info, immobiliarebelliniepecunia[.]online, lamsnajs[.]site, appsabs[.]site, qpps[.]site, lskbd[.]site, serverakp[.]site, wedmail[.]site, 66d68ce73c83226a[.]ngrok[.]app

TYPE	VALUE
URL	hxxps[:]//1drv[.]ms/b/s!AnMKZoF8QfODa92x201yr0GDysk?e=ZnX3Rm, hxxps[:]//moduloj.lamsnajs[.]site/Modulo32[.]jpg

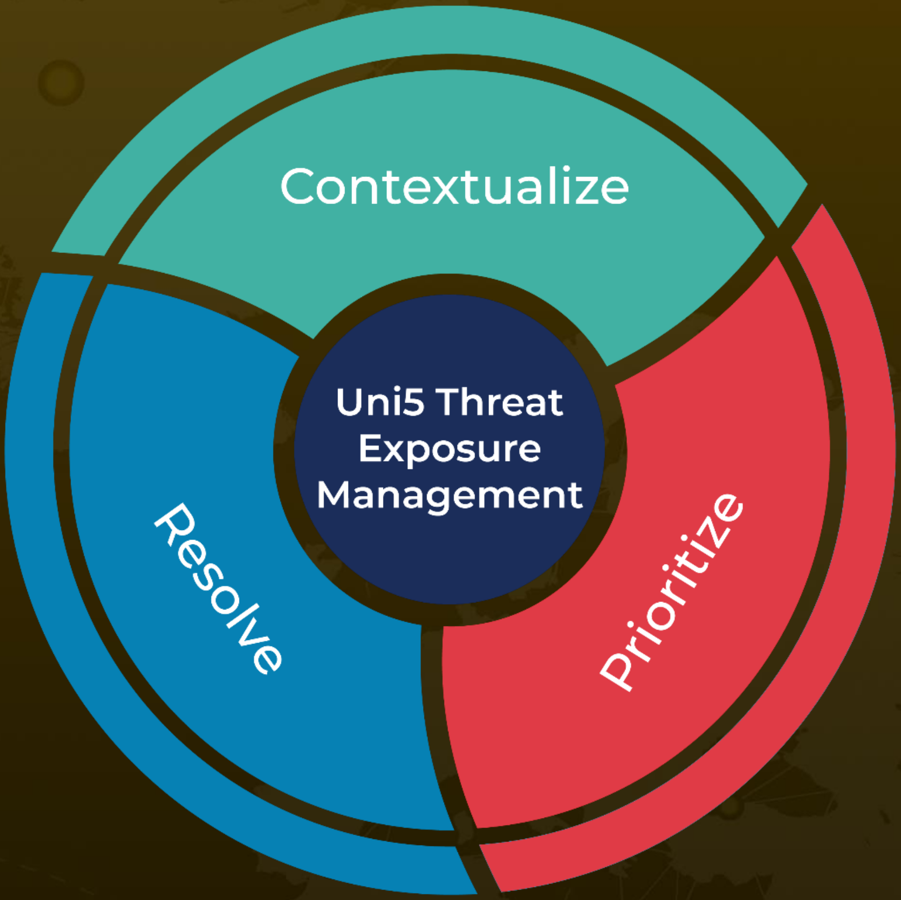
References

https://securelist.com/sambaspy-rat-targets-italian-users/113851/

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, 2024 • 5:00 AM

More at www.hivepro.com