Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

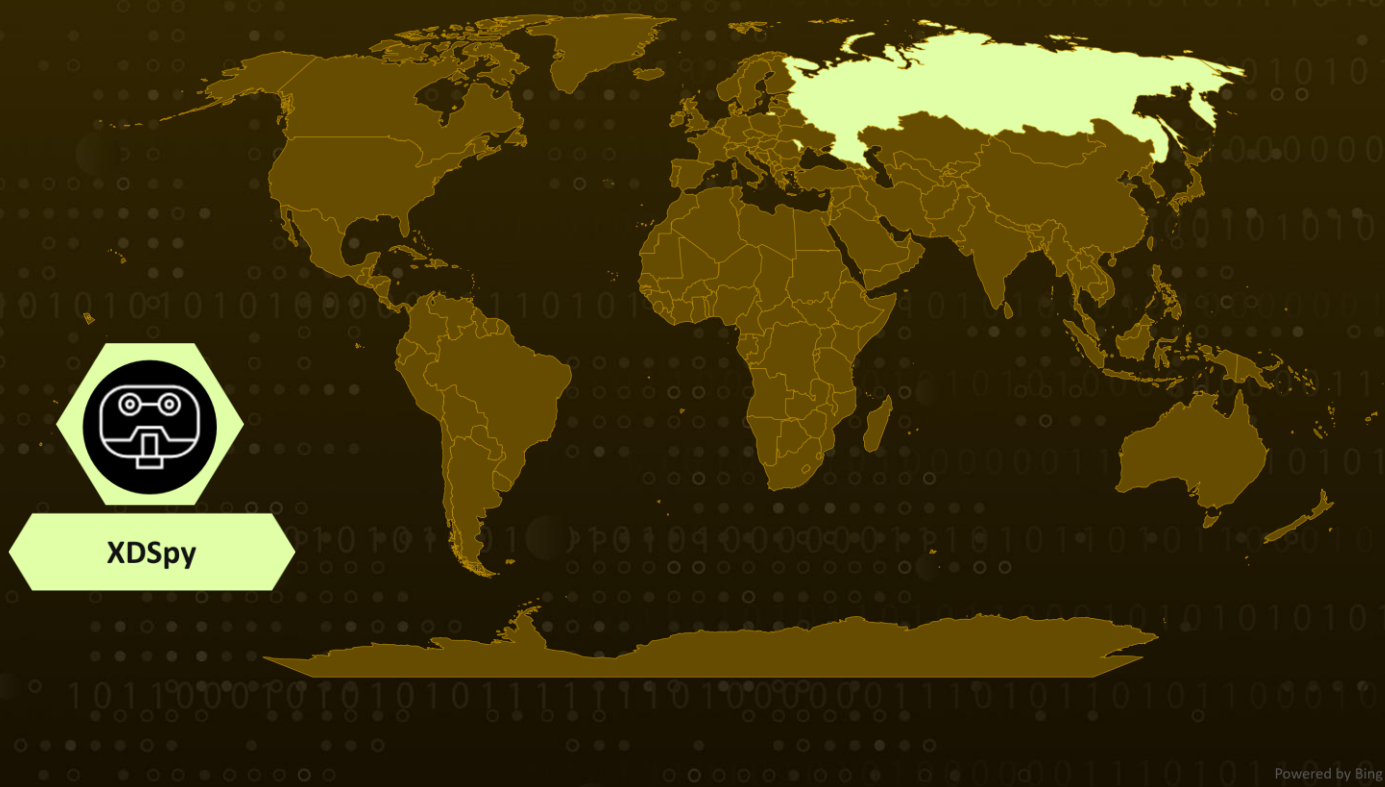
XDSpy Expands Arsenal with New Tool: XDSpy.DSDownloader

Date of Publication	Admiralty Code	TA Number
August 2, 2024	A1	TA2024293

Summary

Attack Discovered: July 2024
Attack Region: Russia and Moldova
Threat Actor: XDSpy (aka UAC-0033)
Malware: XDSpy.DSDownloader
Attack: A phishing campaign orchestrated by the obscure cyber espionage group XDSpy has been targeting entities in Russia. The campaign's victims include a tech company specializing in software for cash registers and an unidentified organization in Transnistria, the Russian-controlled breakaway region in Moldova. The infection chains from this campaign led to the discovery of novel malware known as XDSpy.DSDownloader.

Attack Regions



Attack Details

#1 In July 2024, the XDSpy cyber espionage group initiated a new series of attacks targeting Russian companies. The attackers employed email spoofing to impersonate legitimate senders, increasing the likelihood that recipients would open the phishing emails. These emails contained links that, when clicked, downloaded a RAR archive presumed to contain the XDSpy.DSDownloader malware.

#2 Inside the RAR archive were two executable files in PE32+ format: a legitimate executable and a malicious dynamic link library (DLL) named msi.dll. The attackers used the DLL Side-Loading technique, leveraging the legitimate executable to load and execute the malicious DLL, classified as XDSpy.DSDownloader. This malware is a previously unknown tool used by XDSpy in these attacks.

#3 XDSpy.DSDownloader is a sophisticated piece of malware used by the XDSpy cyber espionage group. It operates by extracting a decoy document from the RCDATA resource and copying both the msi.dll file and a legitimate executable to the "C:\Users\Public" directory. To ensure persistence, it creates a parameter named "{legit_exe_filename}" in the registry key, attaching the malware to system startup.

#4 XDSpy.DSDownloader malware facilitates the download of a next-stage malware payload from a malicious server via a specific link. In previous campaigns, XDSpy has utilized XDDown, a related tool that drops additional plugins for various malicious activities. These plugins are designed to gather system information, enumerate the C: drive, monitor external drives, exfiltrate local files, and collect passwords.

#5 XDSpy is a cyberespionage group that remained largely undetected for more than nine years, despite its recent surge in activity over the past few months. The group primarily focuses on stealing documents from government entities in Eastern Europe and the Balkans. This specific targeting makes XDSpy particularly intriguing and warrants close monitoring. Its long period of stealth, combined with its intensified operations, indicates a sophisticated and persistent threat actor.

Recommendations

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0010 Exfiltration	T1566 Phishing	T1566.002 Spearphishing Link	T1574 Hijack Execution Flow
T1574.002 DLL Side-Loading	T1204 User Execution	T1204.001 Malicious Link	T1140 Deobfuscate/Decode Files or Information
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	a84d557cc726f521354a308436b0620fbe1a051f. 7741436dcaf11e16e330cc52a133b6ef59a12812, 00bde6ad42ef3cbef9f0f0cc054014435432b17c, 02760b55fa69392d99633c271e43108c64c21807, 68d83a5d25d62f0b15912fb70474dd371db1947d
Domains	protej[.]org, nashtab[.]org, general-resources[.]com, sbordokumentov[.]com
IPv4	89[.]114[.]69[.]65, 89[.]114[.]69[.]48, 82[.]221[.]129[.]24, 185[.]56[.]136[.]50, 159[.]100[.]6[.]5
URLs	hxxps://protej[.]org/zpwidnydav/?e&n=bVq7NwlXhjYOMT, hxxps://protej[.]org/zpwidnydav/?e&n=bVq7NwlXhjYOMT, hxxps://protej[.]org/zpwidnydav/?n=wHFbIDNW9YutX, hxxps://nashtab[.]org/biyasqbuk4/?e&n=GuVZoipdI2UIxk, hxxps://nashtab[.]org/pqwebyug3/?n=PDVXCGFwWnCaNv, hxxps://obshchiye-resursy[.]com/zpwidnydav/?e&n=V1Z82iODc5twdu, hxxps://obshchiye-resursy[.]com/zpwidnydav/?n=Jo9EDoZiYATO77, hxxps://sbordokumentov[.]com/snirboubd/?n=vAR1Xp9BG2nStq, hxxps://sbordokumentov[.]com/snirboubd/?n=ygTQMPQdzlcZ9E
File Path	C:\Users\Public\pdf_20240615_00003645.exe, C:\Users\Public\pismo-22-07-2024_0001.exe, C:\Users\Public\msi.dll, %USERPROFILE%\pdf_20240615_00003645.pdf, %USERPROFILE%\pismo-22-07-2024_0001.pdf, C\Users\Public\zwrdntjl.exe, C:\Users\Public\spbbpzmq.exe, C:\Users\Public\yvpxqixd.exe
Registry	[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] pdf_20240615_00003645.exe = "C:\Users\Public\pdf_20240615_00003645.exe“, [HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] pismo-22-07-2024_0001.exe = "C:\Users\Public\pismo-22-07-2024_0001.exe"

TYPE	VALUE
SHA256	45bbe6950cabe649513edbe819440935d6be5a6ef715c01f7a95862225262da0, 03ea832f0b7531026f1d87dc84ec03f65fe11f3e9de032e5e862b70d8cf0d2d8, 65a953a80a0accd3b9a5b0f5c6978dad223273bd4d5ec892737e569c864fc73c, 01d092290e410617eb3369bf3682af186ae8da0937ee90acadba75ee5d4e17e4, 78ba21a60241da65cf65e951773bbfd606402a3bf43acc5201e95220d13e8817
MD5	1c34280a2228793aad681089179ec0b3, 94aab070678e6d84f0287cfedc037300, 2982ac131e49354ec51e645f9db53b40, 0fd1128bc81eca818909d50f9806fd85, 3bd819440fbc91a530c3c659d99564e3

References

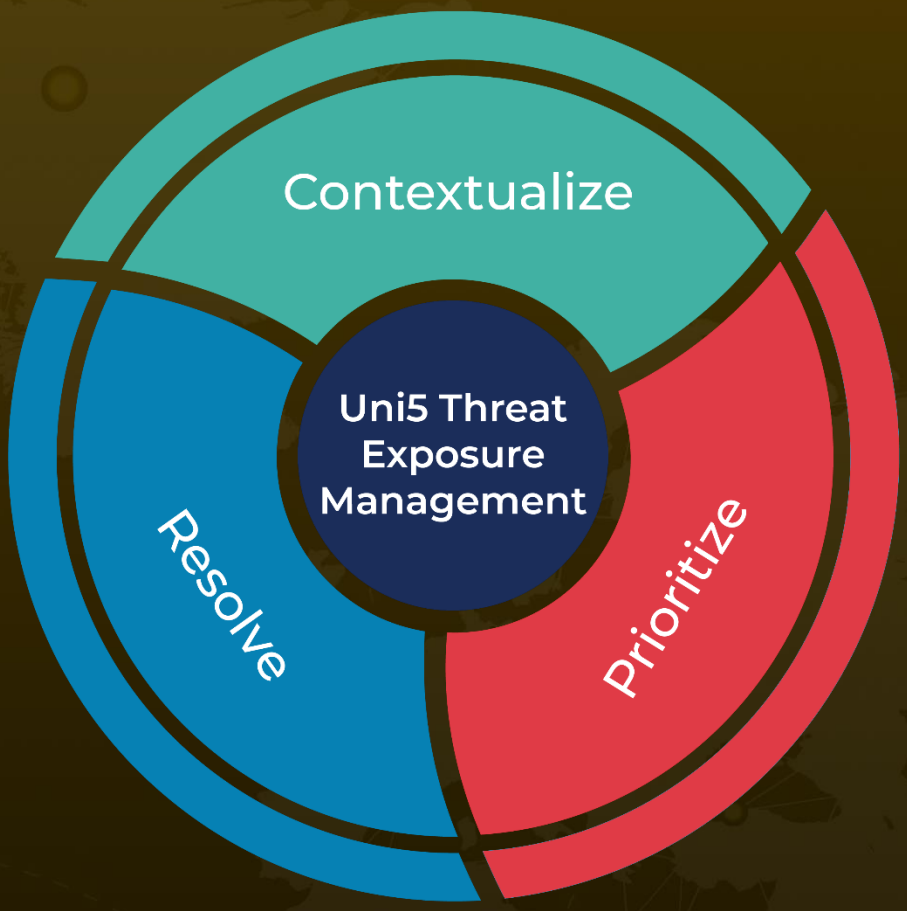
https://habr.com/ru/companies/f_a_c_c_t/news/831420/

https://www.welivesecurity.com/2020/10/02/xdspy-stealing-government-secrets-since-2011/

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

August 2, 2024 • 7:15 AM

More at www.hivepro.com