Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

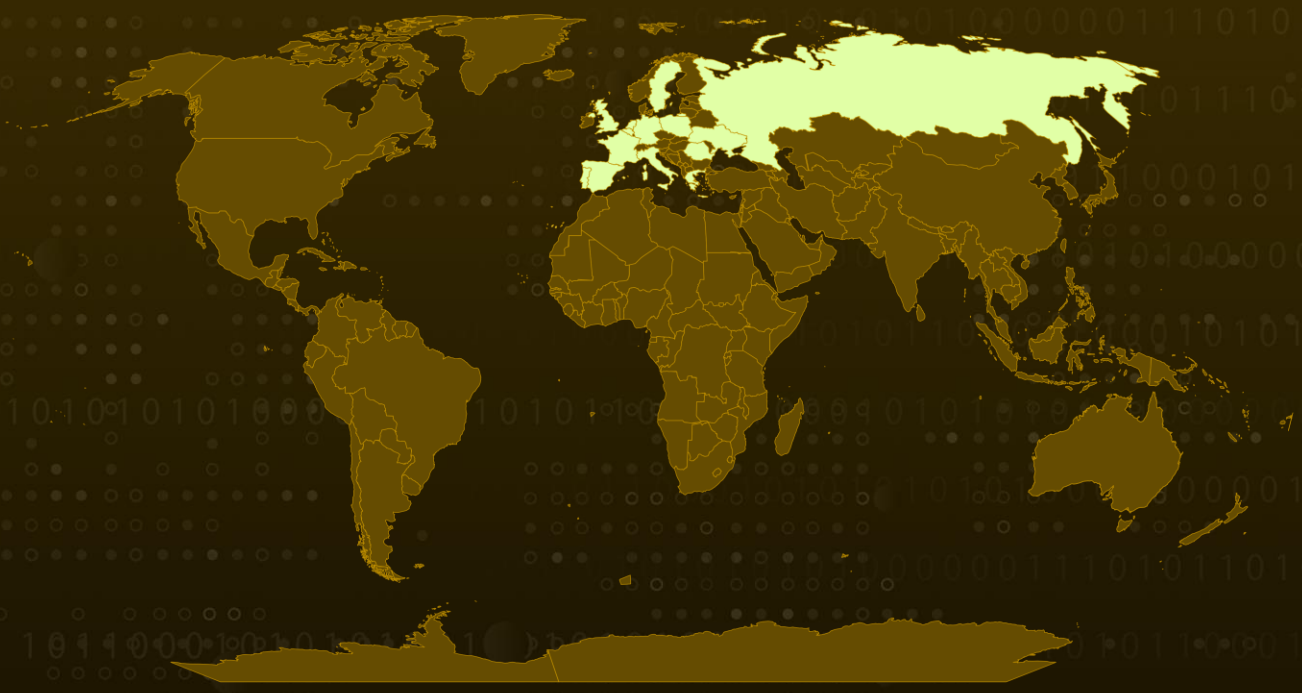
New DBatLoader Malware Campaign Targets European Countries

Date of Publication	Admiralty Code	TA Number
March 30, 2023	A1	TA2023165

Summary

Date: November 2021
Attack Region: European Countries
Targeted Industries: Manufacturing
Malware: DBatLoader, Formbook, Remcos RAT
Attack: A new malware campaign using DBatLoader to target European businesses through phishing emails. The attackers use obfuscation techniques and various file formats to distribute the malware, including Remcos RAT and Formbook.

Attack Regions



Attack Details

#1

A new malware campaign involving DBatLoader, also known as ModiLoader and NatsoLoader, which is being used by threat actors to target various businesses in European countries. The malware payload is distributed through phishing emails that use various tactics to deceive users, including using courier-themed schemes and disguising PDF attachments as Revised Order Documents, Payment Invoices, Quotations, Sales Orders, and similar items. To deliver the payload, the attackers use multilayer obfuscation techniques and various file formats, such as PDF, HTML, ZIP, and OneNote.

#2

The malware campaign distributes two types of malware: Remcos RAT and Formbook. The researchers provide a detailed analysis of DBatLoader's behavior and its attack process, which includes creating a mock trusted directory, using an executable to load the malicious DLL script, and executing PowerShell commands in a BAT script to exclude Microsoft Defender scanning. The article also highlights the use of different file formats and obfuscation methods to avoid detection from antivirus engines.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	**TA0011** Command and Control	**TA0003** Persistence	**TA0009** Collection
TA0005 Defense Evasion	**TA0001** Initial Access	**TA0042** Resource Development	**TA0010** Exfiltration
TA0002 Execution	**T1083** File and Directory Discovery	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information
T1104 Multi-Stage Channels	**T1566** Phishing	**T1548** Abuse Elevation Control Mechanism	**T1105** Ingress Tool Transfer
T1010 Application Window Discovery	**T1016** System Network Configuration Discovery	**T1018** Remote System Discovery	**T1036** Masquerading
T1055 Process Injection	**T1057** Process Discovery	**T1059** Command and Scripting Interpreter	**T1064** Scripting
T1070 Indicator Removal on Host	**T1071** Application Layer Protocol	**T1082** System Information Discovery,	**T1574** Hijack Execution Flow
T1095 Non-Application Layer Protocol	**T1124** System Time Discovery	**T1219** Remote Access Software	**T1497** Virtualization/Sandbox Evasion
T1547 Boot or Logon Autostart Execution	**T1560** Archive Collected Data	**T1562** Impair Defenses	**T1571** Non-Standard Port
T1518 Software Discovery	**T1573** Encrypted Channel	**T1059.001** PowerShell	**T1547.001** Registry Run Keys / Startup Folder
T1070.006 Timestomp	**T1070.004** File Deletion		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	sleda.sleda[.]eu hallowed247.duckdns[.]org Thesquirrelgame[.]net silverline.com[.]sg b-yy[.]xyz
IPV4	185.246.220[.]63
SHA256	6ec341496722bfdde504d430a7ece494701a9369b1fa5376ec488a77ab3c1744 3ddf879ffa91b1bf33eb8d427b6d2dd62cc38e46e5016155556d1502f92c4768
SHA1	d1fcc076d211fca63e5c284178b2d84a6476f8aa 59d3de7748e1090ce95523601224ce5ab6cc4a3a
MD5	fb7dbeea12e4729cf11d6de8588f2b7e f0b7bad0eb081c6b7d3df74e733efd1c ef02ba99d974787a70085537918117c4 eb4f0ea5aea6a1cab3d257cfb04023e2 e7ab3b74689203a229a62b87865f1e7c d9bfe352512b49e002a2744f9d80879a d9844515b7d09d74de188856b60c88c0 d51576e2e216292a72ce16821f9696d3 cdac8ab69c92d012de0650c64be1c335 Cac32da3ef6d2c4551e73ebfafef4393 c1d19535ded9e0ff8e293f6852b24b91 be889f4ab5ce7e99c131463c58205ba0 bc701846e84feb25a355f34194e2a957 b375e74a145c45d07190212e9157e5f8 b2d368435d5896419751add4cc338fc4 b1b76651c4db6ab4742722ce54e38789 b11db475600ad34d68ad26fb30abe498 aa8836fa3879074748f6dca63476aba9 9e7212a41b4885094008bfe2c5e1b54e 85b2a41e98412f2867715c9ae5ad27ac 55aba243e88f6a6813c117ffe1fa5979 4c39cdd2bfb2c7dde761a6e5b8c01321 42d872a2eae6e4f0d171d1f291846e30 3dde7b13d4736c11a67bc8fbad976d37

TYPE	VALUE
MD5	35e8d4c313c7e793a5cc92995147a310 231ce1e1d7d98b44371ffff407d68b59 213c60adf1c9ef88dc3c9b2d579959d2 1d1f8534ee6dbe1dbeade30e912a9136 1d177fccdcc51ad5d20545bd65d9c352 1c19601797e347b2c70c0cd48f7ccd9d 1978b12cacb91b0d0f77a9979db9e671 10904cb6103086d04ba0d76bcf7a65dc 0e8aefd1dade4f059c2881c6e05f689f 04ecfc3fa0c53151d976f2d6fbd65c31 00c168883239c13aa213a5337aca3dae

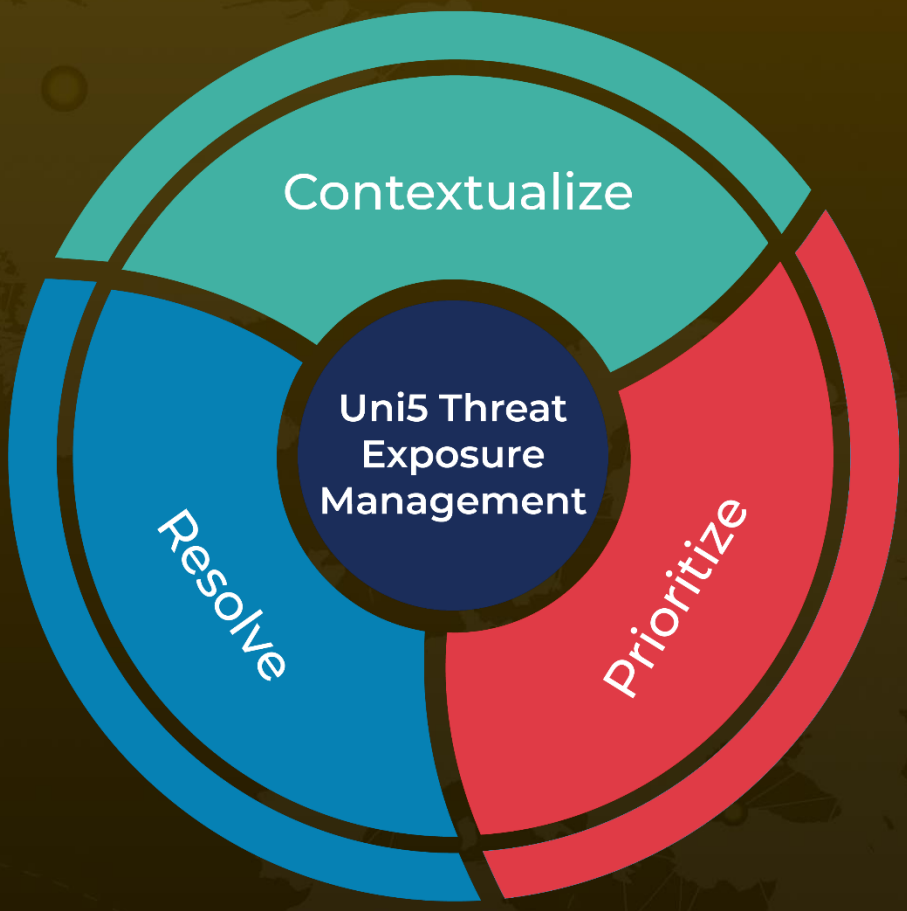
References

https://www.zscaler.com/blogs/security-research/dbatloader-actively-distributing-malwares-targeting-european-businesses

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

March 30, 2023 • 2:30 AM

More at www.hivepro.com