Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

MATA Backdoor Targets Eastern European Industrial Companies

Date of Publication	Admiralty Code	TA Number
October 20, 2023	A1	TA2023427

Summary

First Appearance: August, 2022
Attack Region: Eastern Europe
Affected Platforms: Windows, Linux
Targeted Industries: Oil and gas sector and Defense
Malware: MATA Backdoor
Attack: MATA malware, a sophisticated backdoor framework, updated to target Eastern European industrial companies via spear-phishing, compromising financial software servers, and infiltrating networks, even air-gapped systems, using a complex set of components and sophisticated evasion techniques.

Attack Regions

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2021-40449	Microsoft Windows Win32k Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2021-26411	Microsoft Internet Explorer Memory Corruption Vulnerability	Microsoft Internet Explorer	✓	✓	✓

Attack Details

#1 The MATA malware is a backdoor framework that initially appeared in August 2022 and has been updated for use in targeting industrial companies in Eastern Europe. MATA is written in C++ and the updated version is harder to detect and remove. The attackers employed several methods to evade detection, including a custom loader, encryption and compression techniques, and the use of legitimate system processes.

#2 The attack involved spear-phishing emails and a complex infection chain involving loader, trojan, and stealer components. What's striking is the use of internal IP addresses as Command and Control (C&C) server addresses, suggesting a network of proxy servers.

#3 The attack started by compromising financial software servers, granting access to numerous organization subsidiaries. The attackers progressively infiltrated the network, taking control of the parent company's domain controller, security solutions, and even air-gapped systems. They introduced three new generations of MATA malware, including a Linux variant.

#4 To bridge air-gapped networks, they utilized USB propagation modules and employed various stealers to exfiltrate sensitive data. Furthermore, they used exploits such as CVE-2021-40449, CVE-2021-26411 to bypass security measures.

#5 Spear-phishing emails were used to deliver malicious Word documents to employees in the targeted organizations. These documents contained macros that, when enabled, installed the MATA backdoor on the victim's computer.

#6 Once installed, the MATA backdoor allowed the attackers to remotely control the victim's computer, steal data, and deploy additional malware. This multi-faceted attack campaign highlights the MATA cluster's advanced tactics and their ability to adapt and evolve their malware.

Recommendations

Regular Software Updates: Ensure that all operating systems, software applications, and security solutions are kept up-to-date with the latest patches and updates. This helps eliminate vulnerabilities that adversaries can exploit.

Endpoint Security: Use robust endpoint protection solutions that include antivirus, anti-malware, and behavior-based detection to safeguard individual devices from malware and other threats.

Air-Gapped Network Security: Strengthen the security of air-gapped networks by restricting physical access to USB ports, utilizing intrusion detection systems, and monitoring for any suspicious activity near air-gapped systems.

Multi-Factor Authentication (MFA): Enforce the use of MFA for accessing critical systems and sensitive data. This adds an additional layer of security, making it harder for attackers to gain unauthorized access.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	TA0040 Impact	T1574 Hijack Execution Flow	T1547 Boot or Logon Autostart Execution
T1049 System Network Connections Discovery	T1105 Ingress Tool Transfer	T1136 Create Account	T1021 Remote Services

T1070 Indicator Removal	T1055 Process Injection	T1140 Deobfuscate/Decode Files or Information	T1564 Hide Artifacts
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1587.004 Exploits	T1102 Web Service
T1115 Clipboard Data	T1562 Impair Defenses	T1059 Command and Scripting Interpreter	T1014 Rootkit
T1090 Proxy	T1113 Screen Capture	T1134 Access Token Manipulation	T1056 Input Capture
T1104 Multi-Stage Channels	T1036 Masquerading	T1106 Native API	T1027 Obfuscated Files or Information
T1095 Non-Application Layer Protocol	T1573 Encrypted Channel	T1123 Audio Capture	T1110 Brute Force
T1087 Account Discovery	T1068 Exploitation for Privilege Escalation	T1059.001 PowerShell	T1588.001 Malware

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	a1fc74b7fb105252aba222f5099fbd04, bb93392daece237207b6e32fb5fb4f00, 0818cda2299b358e1ddf4ea59249a6c4, 14fee51bb001abb6ea2c0d8c78863a0d, a6a6d7b87656a0590a12c3ebaa678740, 8f0d45e48d797ac3631b5b572d44b6e8, a88f606a45cea11909fcedadc8945ba7, b29d5a6445140ca3bbdef4f05ea17fd5,

TYPE	VALUE
MD5	b458e336911f092177a64d07b0bf1c76, fed5ff0f9460fea41a8278fffa4c2ddb, e6cc5ba724854702abc7f530d1a8f19c, 6b987944074fda626f8b00751fb9d197, a966668feca72d8dddf3c737d4908a29, b52439640b7f0e0273f0d15bb3af6198, fd7de2b8572f35f0f6f58bba6ff2360e, 4d1e16e2b914243e0c63017676956a73, 0ba8fe6dd895184236618a042bdf835b, 13e9b02b089e9a01ddbe41452d2c409d, 9347abda2aaaefb40aa1e4034a6ded58, ea138d32ce4371d0921cb9f0daead4cb, 01b3c7b2ff7e5158f80f593c09232e04, 996013c565b1f0ae68418d09d712d72b, 5f619927b586a6f776eb582f661ed55c, 91014e9b43ad489535e62e1b048feb59, 289b0d0b626b0be26ee81ed84fb94ec1, 9672437e1dc219ca8a4ee847bed25d0d, 63e7b2fc0a0e6f1db3dee98f4f1dec43, 5c3a88073824a1bce4359a7b69ed0a8d, 2f9e82625774c8051607f791fb9de9b1, 0ef0dfbb4a56cf1d6eff6032ea988162, 09f6c007b16804841a6d02ae87107e3f, fee8d182e6643099523dab41ba1c95b5, 91d04fd26dda91a90fa4169cb251d8ab, 80008a0f7035893d17d7f659e81e716e, 6533e7d5f0f680006031512f8378bfcb, fee3bc01a67339e8eceb9514d8be629c, 3452a24904da2fcf6b79ee1734e9eee1, 15b33a171003fa1a0a24c6ca8f24115a, 2BF250D64E72A14F05EE190148291564, 108854ed57caeeeaeefc20182ea67e94, 94980f93bd9019d84b42104615e86b79
IPv4	185.62.56[.]117, 37.120.222[.]191, 185.25.50[.]199, 85.239.33[.]250,

TYPE	VALUE
Domains	tarzoose[.]com, beeztrend[.]com, cakeduer[.]com, zawajonly[.]com, merudlement[.]com, icimp.swarkul[.]com, mbafleet[.]com, prajeshpatel[.]com, myballmecg[.]com, speclaurp[.]com,

Patch Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40449

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26411

References

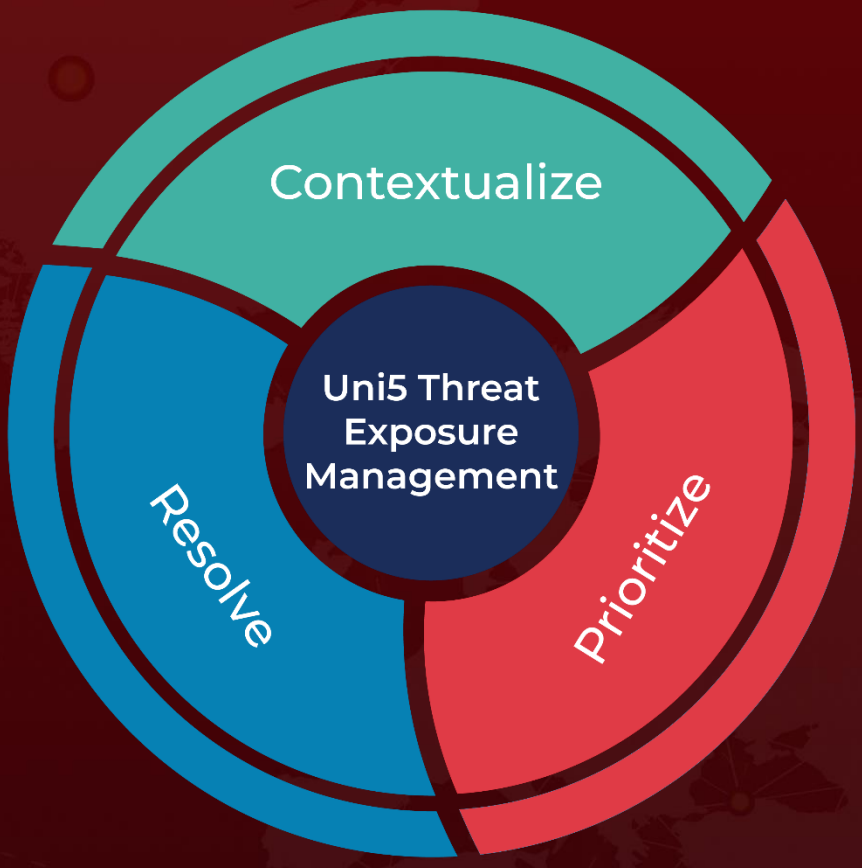
https://securelist.com/updated-mata-attacks-industrial-companies-in-eastern-europe/110829/

https://media.kasperskycontenthub.com/wpcontent/uploads/sites/43/2023/10/18092216/Updated-MATA-attacks-Eastern-Europe_full-report_ENG.pdf

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

October 20, 2023 . 5:00 AM

More at www.hivepro.com