Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

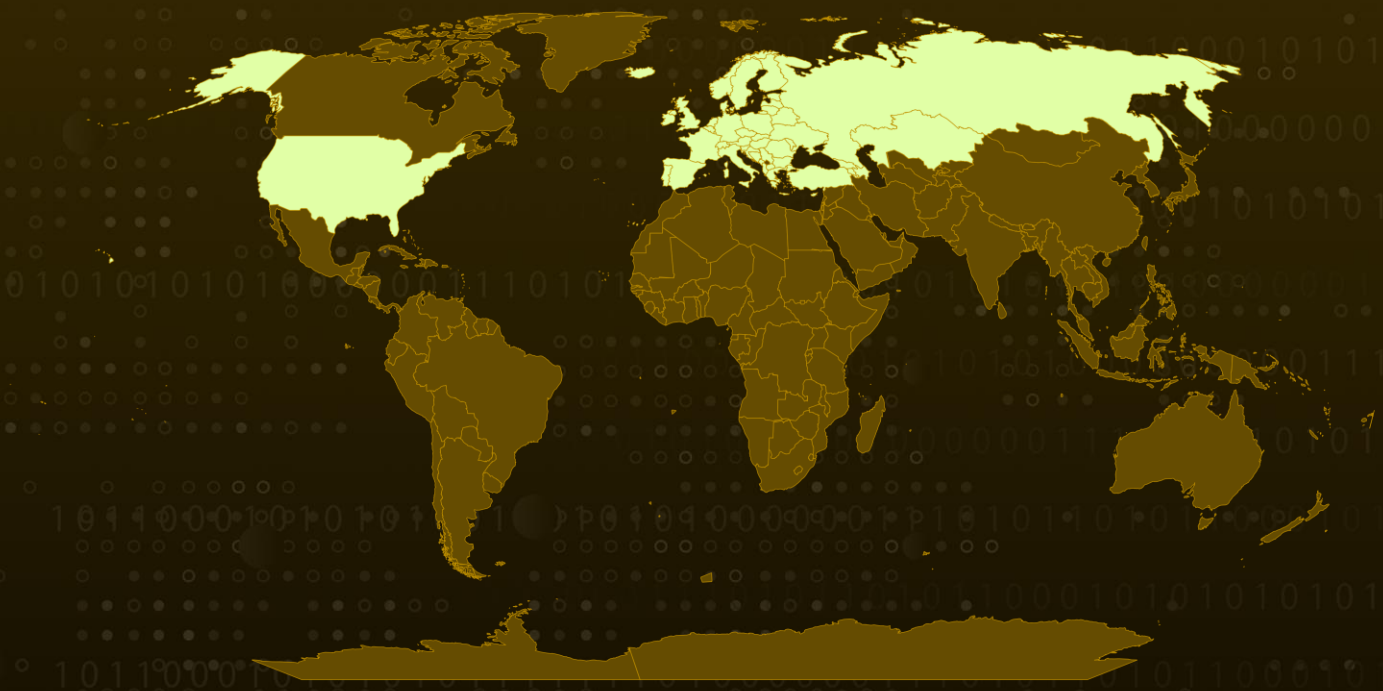
North Korean-Backed Group's Sparks X_Trader Supply Chain Attack

Date of Publication	Admiralty Code	TA Number
April 27, 2023	A3	TA2023203

Summary

Attack Began: March 2023
Malware: X_Trader and Veiledsignal backdoor
Attack Region: Europe and US
Targeted Sector: Energy and Finance
Attack: The X_Trader software supply chain attack affected at least a number of critical infrastructure entities in the United States and Europe.

Attack Regions



Attack Details

#1

Last month's 3CX breach, resulting from the X_Trader software supply chain attack, has also inflicted damage upon multiple critical infrastructure organizations in both the United States and Europe. The Trading Technologies attacks, which could be associated with a North Korean-backed threat group, employed a trojanized X_Trader software installer to launch the VEILEDSIGNAL multi-stage modular backdoor onto the targeted systems.

#2

The infection chain commences with the Trojanized installer labeled as X_TRADER_r7.17.90p608.exe, which comprises a malicious executable called Setup.exe. Subsequently, it drops the Veiledsignal backdoor that can launch harmful shellcode or inject a communication module into the Chrome, Firefox, or Edge processes operating on compromised systems. These consecutive software supply chain compromises illustrate how North Korean operators can effectively exploit network access to develop and distribute malware while navigating between targeted networks, all aligned with North Korea's strategic objectives.

Recommendations

Given the extent of damage caused by the Trojanized X_Trader software, organizations should prioritize strengthening their supply chain security measures to avoid such incidents in the future. It is crucial to conduct regular security assessments of third-party software vendors and ensure that they adhere to industry best practices.

To detect and respond to similar attacks, organizations must implement robust network monitoring capabilities that can identify suspicious activity, such as network intrusions and data exfiltration. Proactive threat intelligence can also provide early warnings of potential supply chain compromises and enable faster response times.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0040** Impact	**TA0042** Resource Development
T1588 Obtain Capabilities	**T1588.004** Digital Certificates	**T1608** Stage Capabilities	**T1608.003** Install Digital Certificate
T1190 Exploit Public-Facing Application	**T1195** Supply Chain Compromise	**T1195.002** Compromise Software Supply Chain	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**T1055** Process Injection	**T1027** Obfuscated Files or Information	**T1036** Masquerading
T1036.001 Invalid Code Signature	**T1070** Indicator Removal	**T1070.001** Clear Windows Event Logs	**T1070.004** File Deletion
T1112 Modify Registry	**T1140** Deobfuscate/Decode Files or Information	**T1497** Virtualization/Sandbox Evasion	**T1497.001** System Checks
T1620 Reflective Code Loading	**T1622** Debugger Evasion	**T1012** Query Registry	**T1082** System Information Discovery
T1083 File and Directory Discovery	**T1614** System Location Discovery	**T1614.001** System Language Discovery	**T1071** Application Layer Protocol
T1071.001 Web Protocols	**T1071.004** DNS	**T1105** Ingress Tool Transfer	**T1573** Encrypted Channel
T1573.002 Asymmetric Cryptography	**T1565** Data Manipulation	**T1565.001** Stored Data Manipulation	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	900b63ff9b06e0890bf642bdfcbfcc6ab7887c7a3c057c8e3fd6fba5ffc8e5d6,6e989462acf2321ff671eaf91b4e3933b77dab6ab51cd1403a7fe056bf4763ba,aa318070ad1bf90ed459ac34dc5254acc178baff3202d2ea7f49aaf5a055dd43,6e11c02485ddd5a3798bf0f77206f2be37487ba04d3119e2d5ce12501178b378,47a8e3b20405a23f7634fa296f148cab39a7f5f84248c6afcfabf5201374d1d1,cc4eedb7b1f77f02b962f4b05278fa7f8082708b5a12cacf928118520762b5e2,277119738f4bdafa1cde9790ec82ce1e46e04cebf6c43c0e100246f681ba184e,cb374af8990c5f47b627596c74e2308fbf39ba33d08d862a2bea46631409539f,d937e19ccb3fd1dddeea3eaaf72645e8cd64083228a0df69c60820289b1aa3c0,e185c99b3d1085aed9fda65a9774abd73ecf1229f14591606c6c59e9660c4345,19442d9e476e3ef990ce57b683190301e946ccb28fc88b69ab53a93bf84464ae,f8c370c67ffb3a88107c9022b17382b5465c4af3dd453e50e4a0bd3ae9b012ce
URL	hxxps[://]www.tradingtechnologies[.]com/trading/order-management
Domain	www.tradingtechnologies[.]

References

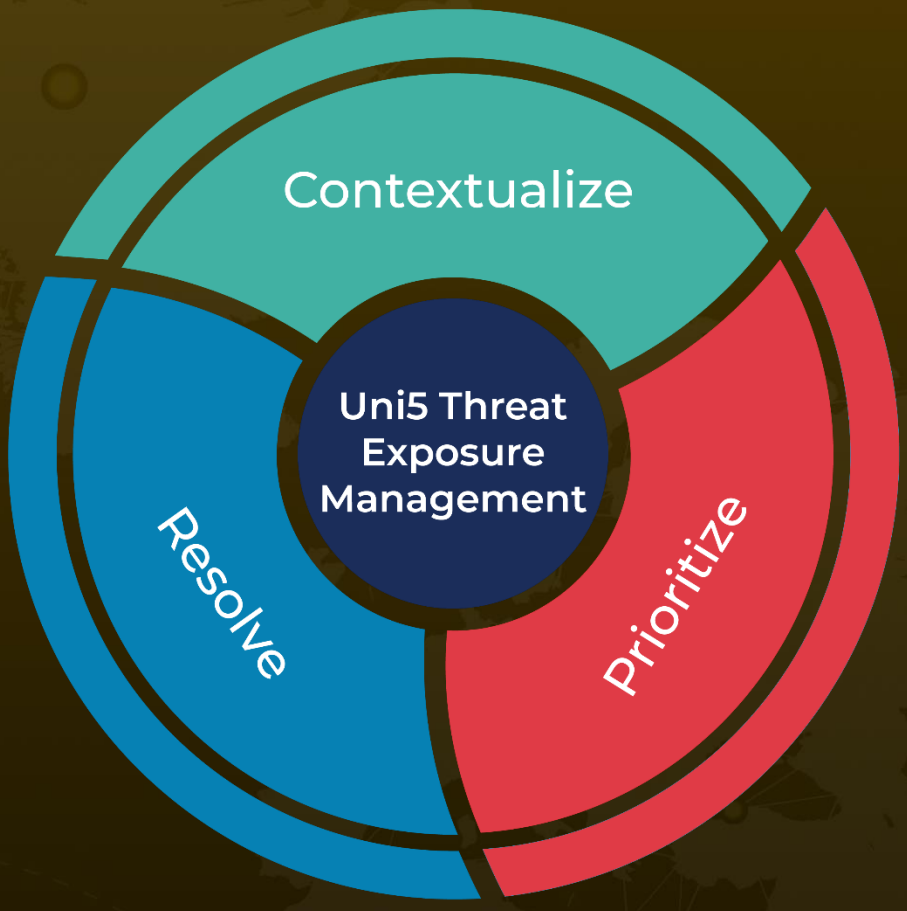
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain

https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

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

April 27, 2023 • 6:31 AM

More at www.hivepro.com