Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Sandworm APT Uses Trojanized KMS Tools to Target Ukrainian Users

Date of Publication	Admiralty Code	TA Number
February 12, 2025	A1	TA2025037

Summary

Attack Discovered: Late 2023
Targeted Country: Ukraine
Affected Platform: Windows
Targeted Industries: Critical Infrastructure, Government
Actor: Sandworm (aka Sandworm Team, Iron Viking, CTG-7263, Voodoo Bear, Quedagh, TEMP.Noble, ATK 14, BE2, UAC-0082, UAC-0113, UAC-0125, FROZENBARENTS, IRIDIUM, Seashell Blizzard, APT 44)
Malware: BACKORDER, DarkCrystal RAT (aka DcRAT), Kalambur backdoor
Attack: The Sandworm cyber-espionage group, linked to the Russian military, is targeting Windows users in Ukraine with trojanized Microsoft Key Management Service (KMS) activators and fake Windows updates to deliver malware. These attacks, which likely began in late 2023, disguise malicious payloads as legitimate system tools to trick users into unknowingly installing malware. As part of this campaign, the attackers have deployed a BACKORDER loader to deliver DarkCrystal RAT (DcRAT) designed for data exfiltration and cyber espionage, allowing them to steal sensitive information, monitor user activity, and maintain persistent access to compromised systems.

Attack Timeline

2015–2016 (BlackEnergy & Industroyer)
Sandworm orchestrated cyberattacks on Ukraine's power grid, causing blackouts in 2015 and 2016.

2017 (NotPetya Ransomware)
Orchestrated the NotPetya attack, initially hitting Ukrainian businesses before expanding worldwide.

2022 (Industroyer2 & HermeticWiper)
During Russia's invasion of Ukraine, Sandworm deployed Industroyer2 to target Ukraine's energy infrastructure and HermeticWiper to erase data from government and corporate networks.

2023 (BACKORDER Malware)
Leveraging trojanized Microsoft KMS activation tools to deliver the BACKORDER

2024 (Espionage campaign)
Sandworm targeted Ukrainian military personnel by spoofing the Army+ app website to distribute malware, enabling covert access and data theft.

2025 (BACKORDER & DcRAT Malware)
Sandworm spreads a new version of BACKORDER, ultimately deploying the DcRAT, via pirated KMS activators and fake Windows updates.

Attack Regions

Attack Details

#1 Sandworm (aka APT44), a Russian state-sponsored cyber espionage group, has been targeting Ukrainian Windows users since late 2023. The group leverages trojanized Microsoft Key Management Service (KMS) activation tools and fake Windows updates to deploy an updated version of their BACKORDER loader. Once executed, this loader facilitates the delivery of Dark Crystal Remote Access Trojan (DcRAT), a powerful malware used for data exfiltration and cyber espionage.

#2 Ukraine's widespread reliance on unlicensed software, with estimates suggesting that up to 70% of software in government and enterprise environments is pirated, has created a massive attack surface. One observed case involved a password-protected ZIP file which was uploaded to a torrent site. Disguised as a KMS activation tool, it contained the BACKORDER loader, specifically designed to target users looking to bypass Windows licensing restrictions.

#3 Since this initial discovery, researchers have linked at least seven separate malware distribution campaigns to this activity, all employing similar lures and attack techniques. The most recent campaign, detected on January 12, 2025, used a typosquatted domain and refined techniques to deliver and execute DcRAT.

#4 When executed, the trojanized activator presents a fake Windows activation interface to deceive users, while the BACKORDER loader silently operates in the background, deploying DcRAT. Once installed, DcRAT establishes a remote connection with an attacker-controlled command-and-control (C2) server. The malware exfiltrates sensitive system data, including credentials and configuration details, while creating multiple scheduled tasks for persistence. Specifically, it registers two tasks using the Windows binary schtasks.exe to execute staticfile.exe with elevated privileges from the AppData directory.

#5 This persistence mechanism ensures that even after a system reboot or user logoff, the malware remains active. This remote administration tool is notorious for its data exfiltration capabilities and has previously been used in Sandworm-led operations. This campaign highlights the inherent risks of using pirated software and underscores the importance of obtaining software from legitimate sources.

Recommendations

- **Use Licensed Software:** Avoid pirated or unlicensed software, as it poses significant security risks. Cybercriminals frequently embed malware in such tools, making them a common attack vector. To ensure system integrity and security, always obtain software from official and trusted sources.
- **Enable Automatic Updates:** Keeping Windows and other software up to date with official security patches is crucial for reducing the risk of exploitation. Regular updates help address vulnerabilities and strengthen system defenses against emerging threats.
- **Verify Software Authenticity:** Before installing any software, especially activation tools or updates, ensure it is legitimate. Always download software directly from official vendor websites to minimize the risk of malware infection.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing	T1204 User Execution
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1218 System Binary Proxy Execution
T1218.011 Rundll32	T1569 System Services	T1569.002 Service Execution	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1548 Abuse Elevation Control Mechanism	T1548.002 Bypass User Account Control	T1562 Impair Defenses
T1562.001 Disable or Modify Tools	T1070 Indicator Removal	T1070.004 File Deletion	T1555 Credentials from Password Stores
T1555.003 Credentials from Web Browsers	T1056 Input Capture	T1056.001 Keylogging	T1082 System Information Discovery
T1021 Remote Services	T1021.001 Remote Desktop Protocol	T1021.004 SSH	T1113 Screen Capture
T1005 Data from Local System	T1090 Proxy	T1090.003 Multi-hop Proxy	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel	T1036 Masquerading

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	172d3750e3617526563dd0b24c4ba88f907622b9
SHA256	afc6131b17138a6132685617aa60293a40f2462dc3a810a4cf745977498e0255, ed5735449a245355706fc58f4b744251f6e499833f02a972f9bd448c28467194, fdc3f0516e1558cc4c9105ac23716f39a6708b8facada3a48609073a16a63c83, 48450c0a00b9d1ecce930eadbac27c3c80db73360bc099d3098c08567a59cdd3, 22c79153e0519f13b575f4bfc65a5280ff93e054099f9356a842ce3266e40c3d, a42de97a466868efbfc4aa1ef08bfdb3cc5916d1accd59cfffff1a896d569412, 8cfa4f10944fc575420533b6b9bbcabbf3ae57fe60c6622883439dbb1aa60369, 8a4df53283a363c4dd67e2bda7a430af2766a59f8a2faf341da98987fe8d7cbd, 70c91ffdc866920a634b31bf4a070fb3c3f947fc9de22b783d6f47a097fec2d8, 0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31a6, 5bff08a6aa7a7541c0b7b1660fd944cec55fa82df6285166f4da7a48b81f776e, 4b9e32327067a84d356acb8494dc05851dbf06ade961789a982a5505b9e061e3, 039c8dd066efa3dd7ac653689bfa07b2089ce4d8473c907547231c6dd2b136ec, 0e58d38fd2df86eeb4a556030a0996c04bd63e09e669b34d3bbc10558edf31a6, 1a1ffcbab9bff4a033a26e8b9a08039955ac14ac5ce1f8fb22ff481109d781a7, 2de08a0924e3091b51b4451c694570c11969fb694a493e7f4d89290ae5600c2c, 4b0038de82868c7196969e91a4f7e94d0fa2b5efa7a905463afc01bfca4b8221, 7c0da4e314a550a66182f13832309f7732f93be4a31d97faa6b9a0b311b463ff, a00beaa5228a153810b65151785596bebe2f09f77851c92989f620e37c60c935, b45712acbadcd17cb35b8f8540ecc468b73cac9e31b91c8d6a84af90f10f29f8,

TYPE	VALUE
SHA256	cd7c36a2f4797b9ca6e87ab44cb6c8b4da496cff29ed5bf727f0699917bae69a, 4b2e4466d1becfa40a3c65de41e5b4d2aa23324e321f727f3ba20943fd6de9e5, 553f7f32c40626cbddd6435994aff8fc46862ef2ed8f705f2ad92f76e8a3af12, d774b1d0f5bdb26e68e63dc93ba81a1cdf076524e29b4260b67542c06fbfe55c, 70cad07a082780caa130290fcbb1fd049d207777b587db6a5ee9ecf15659419f, c5853083d4788a967548bee6cc81d998b0d709a240090cfed4ab530ece8b436e, aadd85e88c0ebb0a3af63d241648c0670599c3365ff7e5620eb8d06902fdde83, 7d92b10859cd9897d59247eb2ca6fb8ec52d8ce23a43ef99ff9d9de4605ca12b, d13f0641fd98df4edcf839f0d498b6b6b29fbb8f0134a6dae3d9eb577d771589, dd7a9d8d8f550a8091c79f2fb6a7b558062e66af852a612a1885c3d122f2591b, 64def4f01bee099c0a95c240d00c1987b2309fd6513830322ae16874c7728714, 41de9ed75aeac48f5c1ca94e5ed64a27227286c93a8df541f35d729f1ec87418
IPv4	5[.]255[.]122[.]118
Domains	Activationsmicrosoft[.]com, kmsupdate2023[.]com, kms-win11-update[.]net, Windowsupdatesystem[.]org, ratiborus2023[.]com, Onedrivestandaloneupdater[.]com, Kalambur[.]net, Windowsdrivepack[.]com, akamaitechcdns[.]com

References

https://blog.eclecticiq.com/sandworm-apt-targets-ukrainian-users-with-trojanized-microsoft-kms-activation-tools-in-cyber-espionage-campaigns

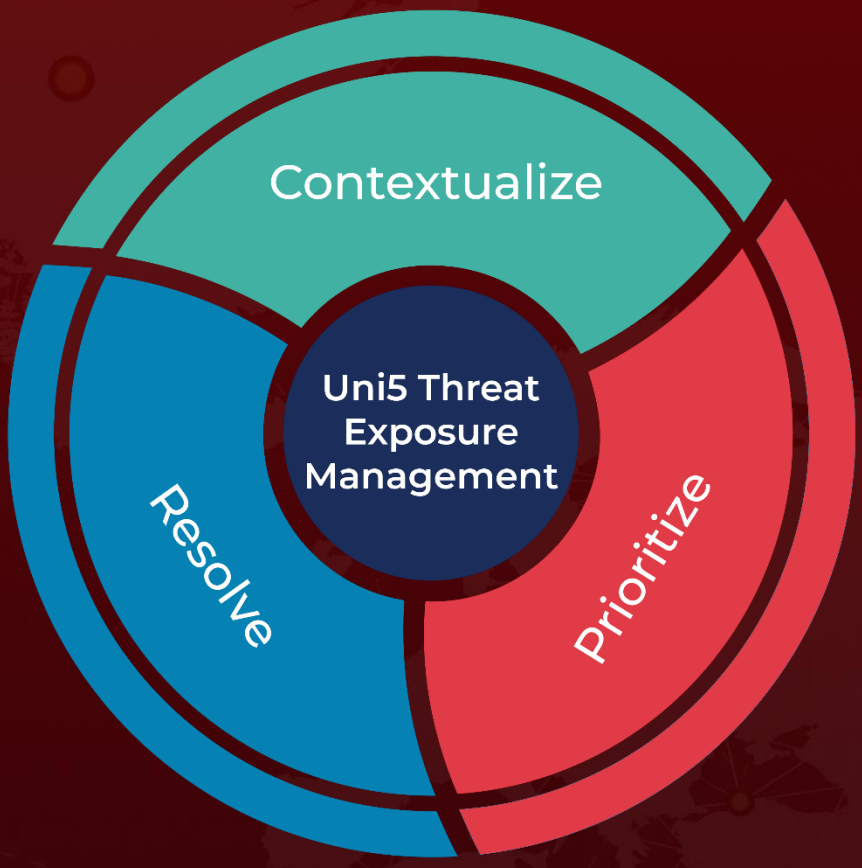
https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

https://therecord.media/ukraine-military-app-espionage-russia-sandworm

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

February 12, 2025 • 7:40 AM

More at www.hivepro.com