Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

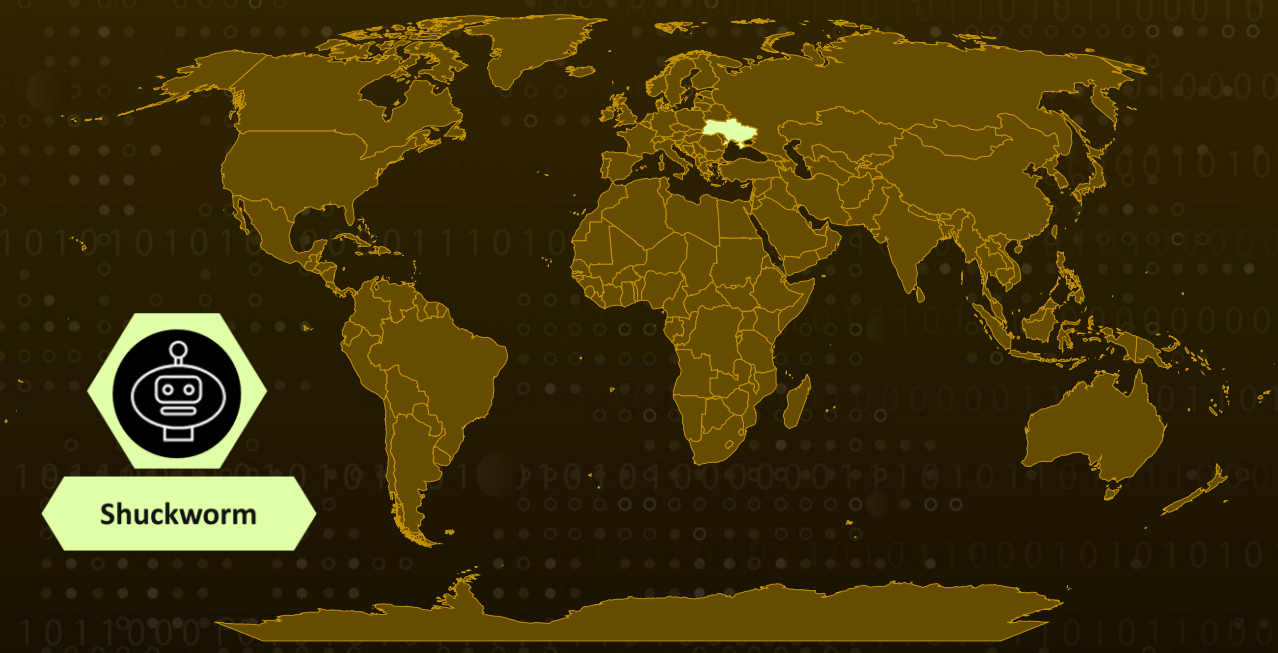
Shuckworm Revives GammaSteel to Spy on Ukraine

Date of Publication	Admiralty Code	TA Number
April 16, 2025	A1	TA2025116

Summary

Attack Discovered: February 2025
Targeted Countries: Ukraine
Targeted Industry: Military
Malware: GammaSteel
Actor: Shuckworm (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Gamaredon, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard)
Attack: A recent cyber-espionage campaign by the Russia-linked Shuckworm group targeted a Western military mission in Eastern Europe, focusing on Ukraine. The attack began in late February 2025 and used an updated version of their GammaSteel malware delivered via a malicious LNK file on a USB drive. The malware leveraged legitimate tools to stay hidden, while storing payloads within the registry to avoid detection. The campaign highlights Shuckworm's evolving tactics and continued focus on intelligence gathering.

Attack Regions



Attack Details

#1 Russia-linked espionage group **Shuckworm** has ramped up its cyber activity once again, zeroing in on Ukraine and the military mission of a Western country based in Eastern Europe. The campaign, which began in late February 2025 and extended into March, relied heavily on an updated version of their custom backdoor known as GammaSteel. In keeping with their long-running strategy, Shuckworm utilized stealthy methods to evade detection shifting from older VBScript-based malware to obfuscated PowerShell payloads, and even using legitimate web services like write.as, cURL, and Tor to exfiltrate data or communicate with their command-and-control (C&C) infrastructure.

#2 The infection appears to have started on February 26, triggered by a malicious LNK file on an external drive. This shortcut file executed a hidden mshta.exe command that launched a highly obfuscated script, which in turn dropped additional files. One of these files, cleverly disguised to resemble a legitimate registry backup, maintained persistent communication with a C&C server. If the server's address wasn't found in a specific registry location, the malware would attempt to resolve it using alternative services, including Cloudflare tunnels.

#3 By March 1, the attackers were actively operating within the network. On one compromised machine, a VBScript was executed via WScript, reaching out to the C&C server using a specially crafted User-Agent string that embedded system details like the username, hostname, and disk serial number. In return, the attackers received and ran obfuscated PowerShell commands, including one that fetched additional scripts designed for reconnaissance capturing screenshots, system information, directory structures, and more. The payload was cleverly stored across various registry keys in an obfuscated format to avoid detection.

#4 Notably, if PowerShell-based exfiltration failed, GammaSteel fell back on using cURL routed through the Tor network to obscure the source of the communication. This resilience in data exfiltration methods, coupled with the rapid move to PowerShell and registry-based payload storage, reflects a growing sophistication in Shuckworm's toolkit.

#5 While not as technically advanced as other Russian APTs, Shuckworm's persistence and evolving tactics make them a persistent threat. Their campaigns consistently focus on Ukrainian entities, likely serving the interests of the Russian Federal Security Service (FSB). This latest operation underscores the group's commitment to espionage and highlights the importance of proactive defense and threat hunting, particularly among high-risk government and military organizations operating in or around Eastern Europe.

Recommendations

- **Check USB Devices and Shortcut Files:** Be careful when using USB drives or other external devices. Turn off auto-run features so files don't open by themselves and keep an eye out for shortcut files (those ending in .lnk) that could be used to launch harmful programs.
- **Keep an Eye on Registry Changes:** Make it a habit to check important registry areas like UserAssist and Console\\WindowsUpdates. If you see unusual or unfamiliar entries, it could be a sign that your system has been tampered with or infected.
- **Lock Down Unnecessary Tools:** If tools like cURL, mshta, or ActiveX aren't needed in your environment, block or restrict their use. These legitimate utilities can be abused by attackers, so using application whitelisting to prevent them from running can help reduce your risk.
- **Educate Users on USB and Phishing Threats:** Make sure users understand the dangers of plugging in unfamiliar USB drives and clicking on suspicious links or files. A quick awareness session can go a long way in preventing malware infections and unauthorized access.
- **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

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0007 Discovery	**TA0005** Defense Evasion	**TA0010** Exfiltration	**TA0011** Command and Control
T1091 Replication Through Removable Media	**T1567** Exfiltration Over Web Service	**T1105** Ingress Tool Transfer	**T1059** Command and Scripting Interpreter

T1059.005 Visual Basic	**T1059.001** PowerShell	**T1132** Data Encoding	**T1132.001** Standard Encoding
T1001 Data Obfuscation	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1547.009** Shortcut Modification
T1218 System Binary Proxy Execution	**T1218.005** Mshta	**T1027** Obfuscated Files or Information	**T1033** System Owner/User Discovery
T1518 Software Discovery	**T1518.001** Security Software Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	714aeb3d778bbd03d0c9eaa827ae8c91199ef07d916405b7f4acd470f9a2a437, 90ec1f4dd69c84c3eb0b2cada4a31168de278eff9b21cb20551ec39d5bcb9da2
Domains	areas-apps-civic-loving.trycloudflare[.]com, des-cinema-democrat-san.trycloudflare[.]com, distributors-marble-saddam-much.trycloudflare[.]com, nav-ni-furnished-handy.trycloudflare[.]com, surfing-programmer-morris-mortality.trycloudflare[.]com, affects-periodic-explorer-broadband.trycloudflare[.]com, abraham-lc-happened-ericsson.trycloudflare[.]com, argentina-references-rapid-selecting.trycloudflare[.]com, beverly-cups-soft-concentrate.trycloudflare[.]com, boxes-harvest-cameroon-uniform.trycloudflare[.]com, cables-tension-bronze-hans.trycloudflare[.]com, convergence-suffering-reel-ingredients.trycloudflare[.]com, detector-excluded-knowledgestorm-two.trycloudflare[.]com, fee-ss-launch-remedies.trycloudflare[.]com, ff-susan-config-mod.trycloudflare[.]com, nail-employed-icon-pre.trycloudflare[.]com, pdt-throwing-pod-places.trycloudflare[.]com, presents-turner-cir-hollow.trycloudflare[.]com, promptly-allows-pendant-close.trycloudflare[.]com, reflection-tomorrow-brook-dakota.trycloudflare[.]com, representatives-liable-sight-tigers.trycloudflare[.]com,

TYPE	VALUE
Domains	sick-netherlands-alumni-electric.trycloudflare[.]com, terry-training-springer-engagement.trycloudflare[.]com, farming-alternatively-velvet-warming.trycloudflare[.]com, pays-habitat-florists-virtually.trycloudflare[.]com, jet-therapy-cape-correctly.trycloudflare[.]com, der-grande-transmitted-benchmark.trycloudflare[.]com, eddie-lewis-exercises-conventions.trycloudflare[.]com, jon-shopzilla-canada-analytical.trycloudflare[.]com, hints-heated-terrain-poem.trycloudflare[.]com, belongs-tells-sum-harvest.trycloudflare[.]com, obj-sudan-quote-aw.trycloudflare[.]com, acquisition-gray-advertisements-trained.trycloudflare[.]com, missouri-itunes-recognize-adds.trycloudflare[.]com, over-function-foo-school.trycloudflare[.]com, criterion-receipt-proceeds-fate.trycloudflare[.]com, phpbb-zealand-hop-magnetic.trycloudflare[.]com, score-adams-coastal-moreover.trycloudflare[.]com Lucystew[.]ru, position.crudoes[.]ru, www[.]phlovel[.]ru
IPV4	3[.]73[.]33[.]225, 107[.]189[.]19[.]137, 107[.]189[.]19[.]218, 165[.]232[.]153[.]27, 172[.]104[.]187[.]254, 64[.]23[.]190[.]235, 85[.]92[.]111[.]12, 45[.]61[.]166[.]43, 159[.]223[.]50[.]199, 139[.]59[.]136[.]192, 104[.]16[.]230[.]132, 104[.]16[.]231[.]132
File path	ntuser.dat.ini

References

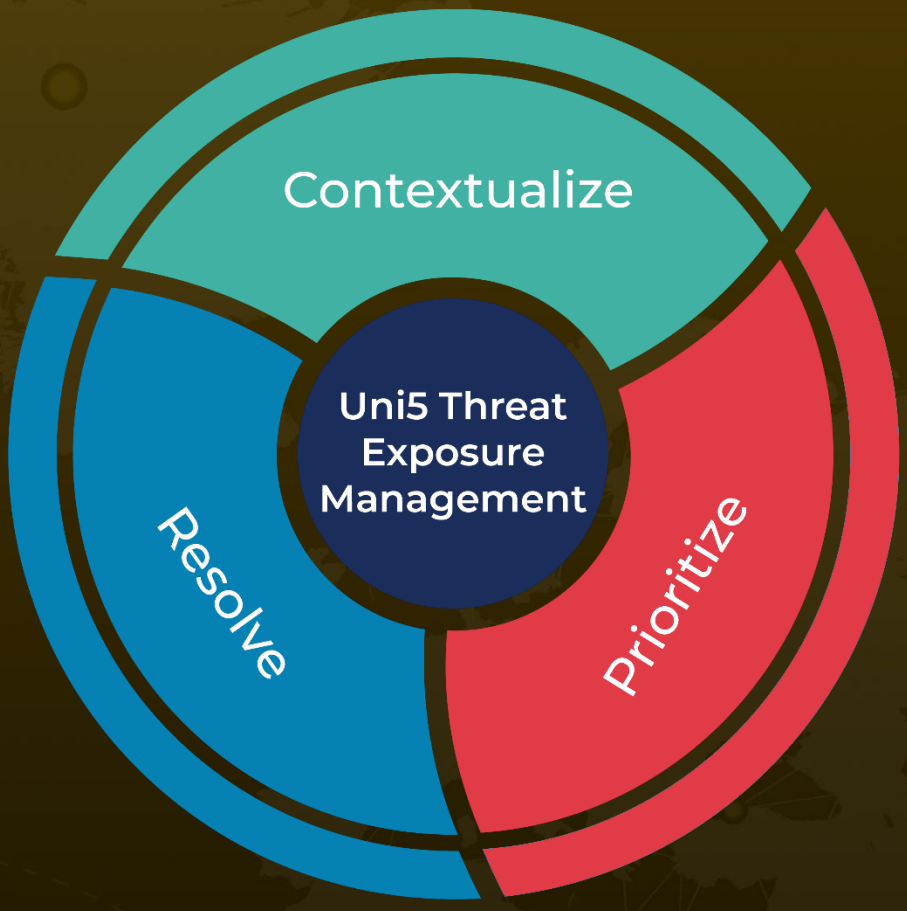
https://www.security.com/threat-intelligence/shuckworm-ukraine-gammasteel

https://www.hivepro.com/threat-advisory/gamaredon-deploys-litterdrifter-usb-worm-in-cyber-espionage-operations/

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 16, 2025 • 1:35 AM

More at www.hivepro.com