Graphiron: New Russian Information Stealing Malware Deployed Against Ukraine

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nodaria-ukraine-infostealer

Russia-linked Nodaria group has deployed a new threat designed to steal a wide range of information from infected computers.

The Nodaria espionage group (aka UAC-0056) is using a new piece of information stealing malware against targets in Ukraine. The malware (Infostealer.Graphiron) is written in Go and is designed to harvest a wide range of information from the infected computer, including system information, credentials, screenshots, and files.

The earliest evidence of Graphiron dates from October 2022. It continued to be used until at least mid-January 2023 and it is reasonable to assume that it remains part of the Nodaria toolkit.

Graphiron functionality

Graphiron is a two-stage threat consisting of a downloader (Downloader.Graphiron) and a payload (Infostealer.Graphiron).

The downloader contains hardcoded command-and-control (C&C) server addresses. When executed, it will check against a blacklist of malware analysis tools by checking for running processes with the names listed in Table 1.

Process names
BurpSuite, BurpSuiteFree, CFF Explorer, Charles, DumpIt, Fiddler, HTTPDebuggerSVC, HTTPDebuggerUI, HookExplorer, Immunity, ImportREC, LordPE, MegaDumper, NetworkMiner, PEToolW, Proxifier, RAMMap, RAMMap64, ResourceHacker, SysInspector, WSockExpert, WinDump, Wireshar, agent.py, autoruns, autoruns, dbgview, disassembly, dumpcap, filemon, httpdebugger, httpsMon, ida,idag, idag64, idaq, idaq64, idau, idau64, idaw, idaw64, joeboxcontrol, joeboxserver, mitmdump, mitmweb, ollydbg, pestudio, proc_analyzer, processhacker, procexp, procexp64, procmon, procmon64, protection_id, pslist, reconstructor, regmon, reshacker, rpcapd, scylla, scylla_64, scylla_86, smsniff, sniff_hit, tcpvcon, tcpview, tshark, vmmat, windbg, x32dbg, x64dbg, x96dbg

Table 1: Graphiron checks against a blacklist of malware analysis tools by checking for running processes with specific names

If no blacklisted processes are found, it will connect to a C&C server and download and decrypt the payload before adding it to autorun.

The downloader is configured to run just once. If it fails to download and install the payload it won't make further attempts nor send a heartbeat.

Graphiron uses AES encryption with hardcoded keys. It creates temporary files with the ".lock" and ".trash" extensions. It uses hardcoded file names designed to masquerade as Microsoft office executables: OfficeTemplate.exe and MicrosoftOfficeDashboard.exe

The payload is capable of carrying out the following tasks:

- Reads MachineGuid
- Obtains the IP address from https://checkip.amazonaws.com
- Retrieves the hostname, system info, and user info
- Steals data from Firefox and Thunderbird
- Steals private keys from MobaXTerm.
- Steals SSH known hosts
- Steals data from PuTTY

- Steals stored passwords
- Takes screenshots
- Creates a directory
- Lists a directory
- Runs a shell command
- Steals an arbitrary file

Password theft is carried out using the following PowerShell command:

[void]
[Windows.Security.Credentials.PasswordVault,Windows.Security.Credentials,ContentType=WindowsRuntime];$vault = New-Object Windows.Security.Credentials.PasswordVault;$vault.RetrieveAll() | % { $_.RetrievePassw

ord();$_} | Select UserName, Resource, Password | Format-Table –HideTableHeaders

The following command was used to export the list of PuTTY sessions:

"CSIDL_SYSTEM\reg.exe" query HKCU\Software\SimonTatham\Putty\Sessions

Similarity to older tools

Graphiron has some similarities with older Nodaria tools such as GraphSteel and GrimPlant. GraphSteel is designed to exfiltrate files along with system information and credentials stolen from the password vault using PowerShell. Graphiron has similar functionality but can exfiltrate much more, such as screenshots and SSH keys.

In addition to this, as with earlier malware, Graphiron communicates with the C&C server using port 443 and communications are encrypted using the AES cipher.

Malware	Go version	Internal name	Obfuscation	Libraries used
Infostealer.Graphiron	1.18	n/a	yes	jcmturner/aescts, buger/jsonparser, golang/protobuf, kbinani/screenshot, lxn/win, mattn/go-sqlite, tidwall/gjson, anmitsu/go-shlex
Downloader.Graphiron	1.18	n/a	yes	jcmturner/aescts
GraphSteel	1.16	Elephant	no	buger/jsonparser, aglyzov/charmap, denisbrodbeck/machineid, gorilla/websocket, jcmturner/aescts, matn/go-sqlite, tidwall/gjson
GrimPlant	1.16	Elephant	no	jcmturner/aescts, denisbrodbeck/machineid, golang/protobuf, kbinani/screenshot, lxn/win, anmitsu/go-shlex

Table 2: Comparison between Graphiron and older Nodaria tools (GraphSteel and GrimPlant)

Nodaria

Nodaria has been active since at least March 2021 and appears to be mainly involved in targeting organizations in Ukraine. There is also limited evidence to suggest that the group has been involved in attacks on targets in Kyrgyzstan. Third-party reporting has also linked the group to attacks on Georgia.

The group sprang to public attention when it was linked to the WhisperGate wiper attacks that hit multiple Ukrainian government computers and websites in January 2022. When WhisperGate was initially loaded onto a system, the malware would overwrite the portion of the hard drive responsible for launching the operating system when the machine is booted up with a ransom note demanding $10,000 in Bitcoin. However, this was just a decoy as the WhisperGate malware destroys data on an infected machine and it cannot be recovered, even if a ransom is paid.

The group's usual infection vector is spear-phishing emails, which are then used to deliver a range of payloads to targets. Custom tools used by the group to date include:

- Elephant Dropper: A dropper
- Elephant Downloader: A downloader
- SaintBot: A downloader
- OutSteel: Information stealer
- GrimPlant (aka Elephant Implant): Collects system information and maintains persistence
- GraphSteel (aka Elephant Client): Information stealer

Like Graphiron, many of Nodaria's earlier tools were written in Go. Graphiron appears to be the latest piece of malware authored by the same developers, likely in response to a need for additional functionality. While GraphSteel and GrimPlant used Go version 1.16, Graphiron uses version 1.18, confirming it is a more recent development.

While Nodaria was relatively unknown prior to the Russian invasion of Ukraine, the group's high-level activity over the past year suggests that it is now one of the key players in Russia's ongoing cyber campaigns against Ukraine.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

SHA-256:

0d0a675516f1ff9247f74df31e90f06b0fea160953e5e3bada5d1c8304cfbe63 — Downloader.Graphiron

878450da2e44f5c89ce1af91479b9a9491fe45211fee312354dfe69e967622db — Downloader.Graphiron

80e6a9079deffd6837363709f230f6ab3b2fe80af5ad30e46f6470a0c73e75a7 — Infostealer.Graphiron

eee1d29a425231d981efbc25b6d87fdb9ca9c0e4e3eb393472d5967f7649a1e6 — Infostealer.Graphiron

f0fd55b743a2e8f995820884e6e684f1150e7a6369712afe9edb57ffd09ad4c1 — Infostealer.Graphiron

f86db0c0880bb81dbfe5ea0b087c2d17fab7b8eefb6841d15916ae9442dd0cce — Infostealer.Graphiron

Network:

208.67.104[.]95 — C&C server