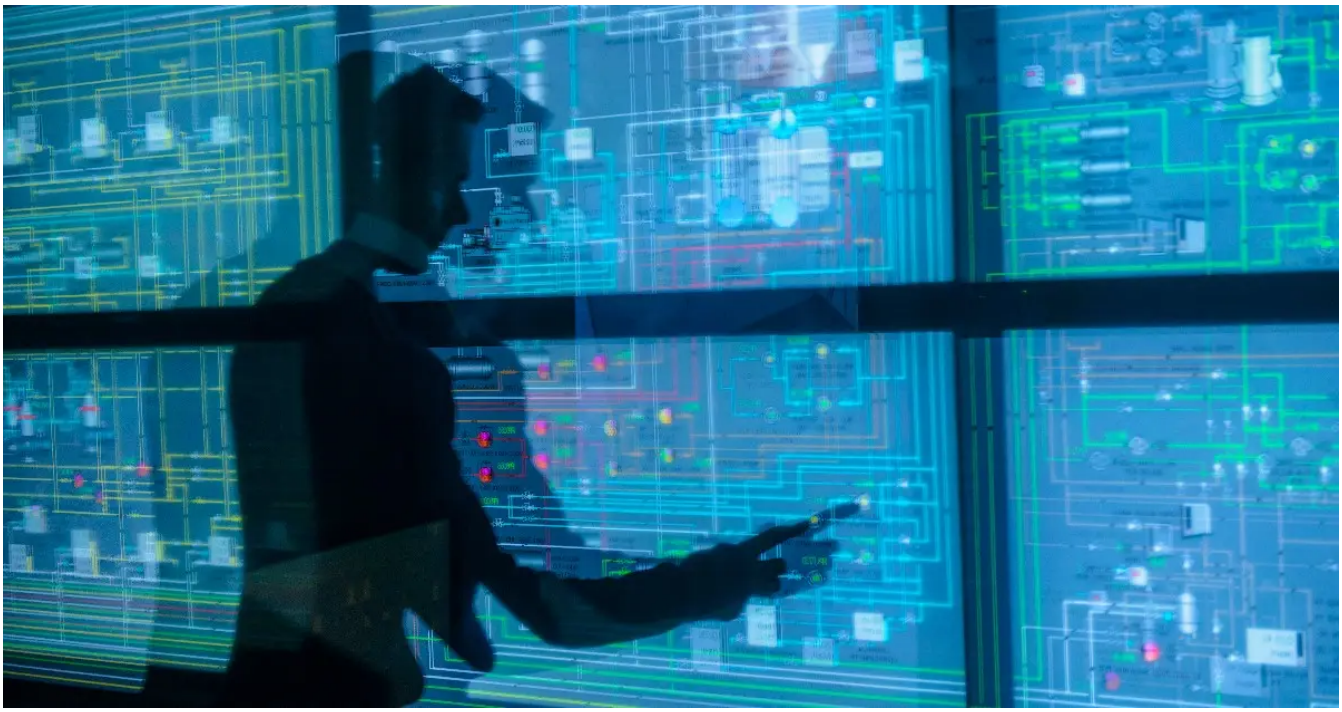
New Hive0117 phishing campaign imitates conscription summons to deliver DarkWatchman malware

securityintelligence.com/x-force/new-hive0117-phishing-campaign-imitates-conscription-summons-deliver-darkwatchman-malware/



Light Dark

September 7, 2023 By Claire Zaboeva
Melissa Frydrych
Golo Mühr
8 min read

IBM X-Force uncovered a new phishing campaign likely conducted by Hive0117 delivering the fileless malware DarkWatchman, directed at individuals associated with major energy, finance, transport, and software security industries based in Russia, Kazakhstan, Latvia, and Estonia. DarkWatchman malware is capable of keylogging, collecting system information, and deploying secondary payloads.

Imitating official correspondence from the Russian government in phishing emails aligns with previous Hive0117 campaigns delivering DarkWatchman malware, and shows a possible significant effort to induce a sense of urgency as the emails reference then-recent amendments regarding conscription. Under the new ordinance, the state will bar individuals who fail to report for service from applying for loans, conducting real estate transactions, engaging in international travel, and suspend their driver's license.

It is highly likely Hive0117 pose a threat to in-region entities and enterprises, given the use of emergent policies associated with the ongoing conflict in Ukraine to conduct operations, combined with the diverse functionality and fileless nature of DarkWatchman malware.

Key findings

- Hive0117 leverages new digital policies associated with Russian mobilization targeting Russian speakers.

- Phishing emails imitate electronic conscription notices from a non-existent military commissariat to deliver fileless DarkWatchman malware.
- Use of the ongoing regional conflict likely signals Hive0117 operations leverage current events to conduct illicit activity.
- The DarkWatchman RAT uses fileless behavior to maintain a footprint on infected systems and may be used to deploy secondary payloads.
- The fileless nature of the DarkWatchman malware, its use of JavaScript and a keylogger written in C#, as well as the ability to remove traces of its existence on compromised systems, are evidence of somewhat sophisticated capabilities.

Email campaign

Following President Vladimir Putin's announcement of 'partial mobilization,' an estimated 900,000 Russian citizens fled the Russian Federation to avoid conscription into the Russian Armed Forces. In response, the Russian government introduced a bill in 2023 that aimed to address the issue of citizens avoiding service and receipt of a physical summons by allowing for the delivery of digital summons via the Gosuslugi — an electronic state services portal.

The emails are directed at work email addresses of individuals associated with several industries based in Russia, Kazakhstan, Latvia, and Estonia, and leveraging an electronic summons for conscription into the Russian Armed Forces as the phishing lure. Hive0117 actors sent Russian-language emails with subject lines appearing to be Orders for Mobilization as of 10 May 2023 (Мобилизационное предписание №291-76005-23 от 10.05.2023).

For authenticity, the emails include multiple images along with logos of the official coat of arms of the Russian Ministry of Defense. Machine translation of the email shows references to the then-recent legislation regarding guidance surrounding mobilization to the Russian Armed Forces.

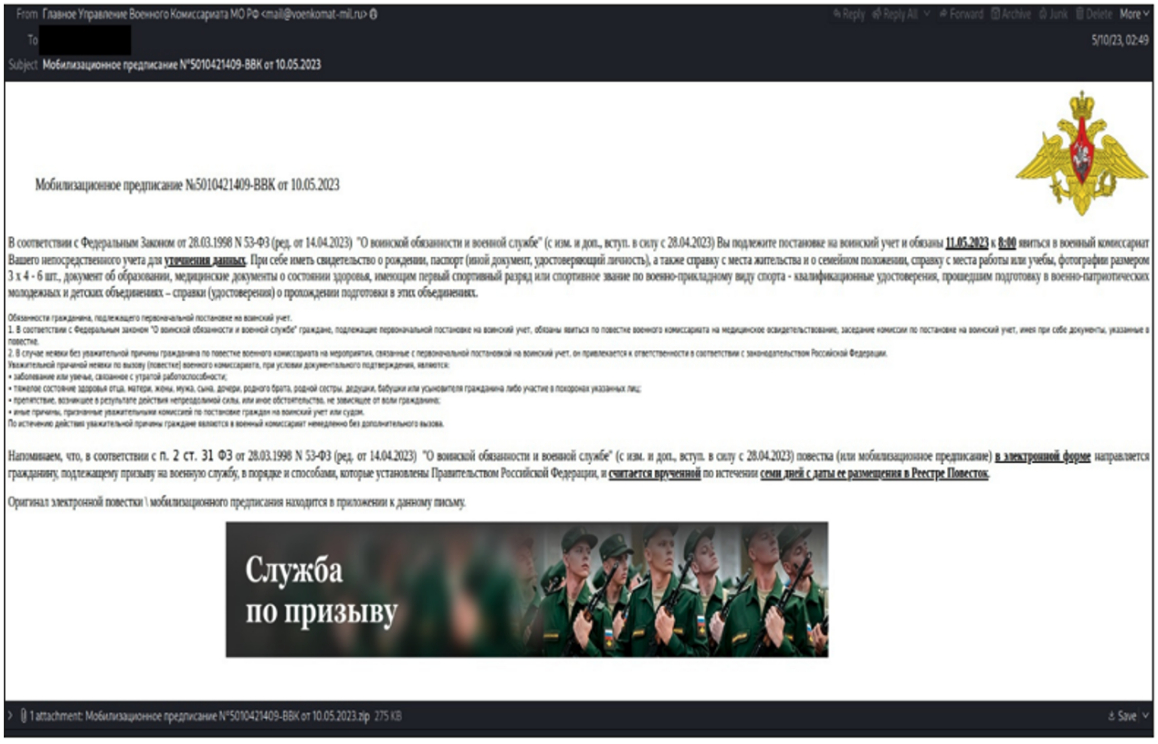


Figure 1: Image of Hive0117 phish imitating electronic conscription notice

Each phishing email contains an archive attachment with a title echoing the email's subject line, combined with an apparent serial number, and the date (Мобилизационное предписание №291-76005-23 от 10.05.2023.zip). The email sender is a fictional organization of the Main Directorate of the Military Commissariat of the Ministry of Defense

of the Russian Federation (Главное Управление Военного Комиссариата МО РФ). Likewise, the same commissariat language (voenkomat) is also included in the visible actor-controlled return path (mail@voenkomat-mil[.]ru).

Additionally, X-Force uncovered reports from Russian publications indicating exact copies of the phishing emails were received by residents and government institutions across Russia, from Nizhny Tagil and Voronezh, to the Amur region, Ulyanosk, Samara, Krasnodar, and Moscow. Reader comments within the articles suggest recipients included the Editorial Office of the Academy of Sciences, the Moscow Post Office, and personnel departments in Moscow.


БЕЗФОРМАТА Nizhny Tagil ▾ Choose a rubric ▾

Main | Archive | Sources | Weather | Incidents | fires | On the water

Viral "summons" to the draft board began to come to e-mail residents of Nizhny Tagil

Photo: mstrok.ru

Today, May 10, by email Tagilian Fake mobilization orders began to arrive en masse from supposedly " **Main Directorate of the Military commissariat Ministry of Defense of the Russian Federation** ". In a document referring to the law " About military duty and military service » The addressee is urged to come to the military commissariat on May 11 by 08:00 to clarify the data. Such a letter was also sent to the email address of the editorial office of the Academy of Sciences " Between the lines».

The document specifies that you must have a birth certificate, passport or other identification document with you. They also ask you to take with you a certificate from the place of residence and marital status, a document from the place of work or study, six photographs 3 by 4 cm in size, a document on education, medical certificates on the state of health and available certificates of participation in military-patriotic youth and children's organizations. In addition, the suspicious letter contains the original email notification. However, the attached zip file could not be downloaded due to anti-virus alerts about a possible threat.

Today, fake subpoenas have begun to arrive in other regions of Russia. As the editors explained Teleport.rf » in the military commissariat of the Amur region, mobilization orders are not sent by e-mail. In addition, such a letter does not indicate to whom it is addressed, and in the sender column a link is given to a non-existent structure - " **Main Directorate of the Military Commissariat of the Ministry of Defense of the Russian Federation** ". Most likely, the attached file contains a dangerous computer virus, it is not recommended to open the application.

РЕКЛАМА ГК ЛИГАЛ p.gk-legal.ru Опытный

Figure 2: Image of local Russian newspaper reporting on the residents receiving fake mobilization orders

Given the contents of the email and their widespread distribution, it is highly likely Hive0117 directed this activity toward both in-country Russian citizens and those residing in Russia's pronounced near abroad.

Malware

The email archive file attachments contain an executable, ultimately installing DarkWatchman malware that functions similarly to the Hive0117 malware reported in April 2022. A full DarkWatchman malware analysis report can be found on IBM X-Force Exchange.

Infection chain

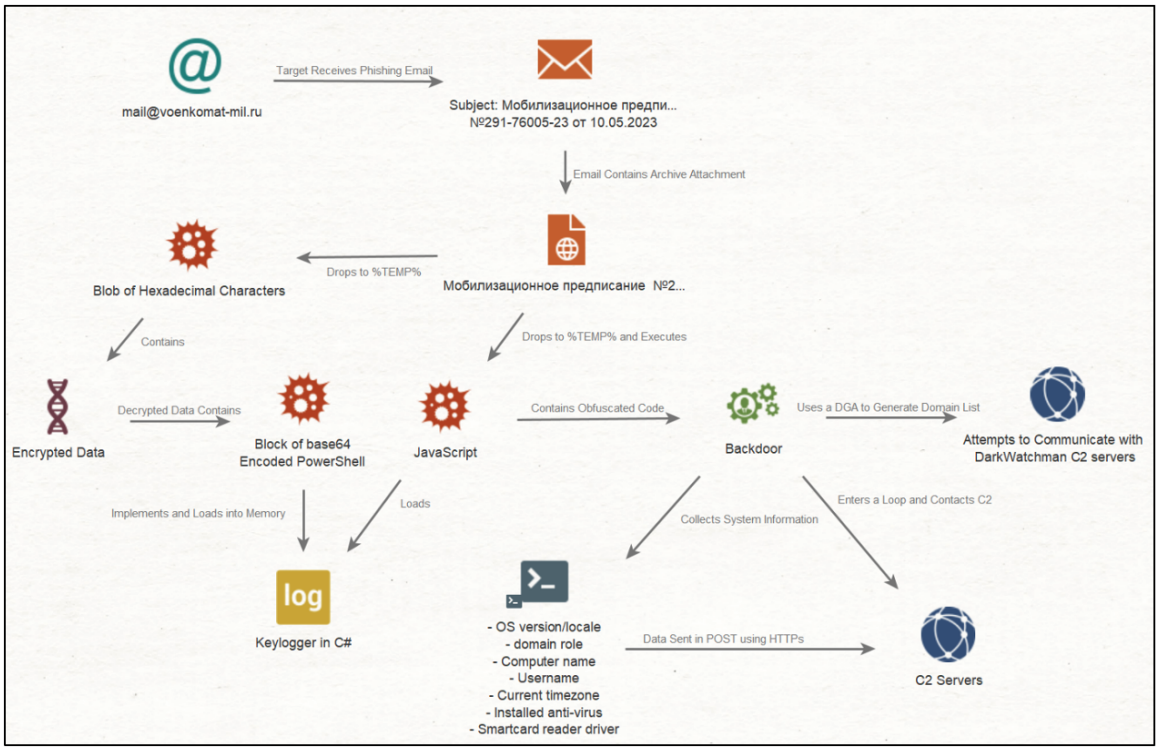


Figure 3: DarkWatchman Malware infection chain

The downloader files, which contact various domains, download files to the %TEMP% location, where a self-extracting archive (SFX) installer drops two files: a JS file and a file containing a blob of hexadecimal characters. The SFX file executes the JS with the SFX file's path as the argument. The JS file contains obfuscated code that functions as the backdoor, and the blob contains encrypted data that when decrypted, contains a block of base64 encoded PowerShell that implements a keylogger. The configuration contains a comment in Russian text, which translates to "The comment below contains SFX script commands" (;Расположенный ниже комментарий содержит команды SFX-сценария), indicating that the author of the malware is a Russian-language speaker, likely based in, or originating from, a Russian-speaking territory.

The SFX archives also drop and register the dynwrapx.dll library, which can be used to call WinAPI functions exported from system DLLs, directly from malicious scripts such as JS or VBS. This allows threat actors to deploy advanced payloads as scripts, without having to rely on executables that would be dropped to disk for execution.

The JavaScript backdoor is executed using the Windows Script Host (WSH) environment, **wscript.exe**, and utilizes the Windows Registry as a storage mechanism for configuration and other data to avoid writing to disk and avoid detection by anti-virus software. In particular, the keylogger is stored in the Registry in an encoded form until executed.

Hive0117 generates a UID string each time it starts that is used as an identifier for various purposes. The UID is calculated based on the C: volume serial number, which is queried and then converted to lowercase characters and padded with zeros (before the serial number) as needed to make the UID string 8 characters long.

Several registry entries are used to store data, such that HKEY_CURRENT_USER\Software\Microsoft\Windows\DWM\ is used as the base for this storage area. Each Registry value is identified using the UID and an alpha-numeric character representing a configuration key **<uid> <config_key>** and contains various configuration and other data (e.g., key log, etc.) previously used by Hive0117.

Executing the backdoor with the name of the SFX file as a parameter will cause an installation routine to be executed. As part of the installation routine, the backdoor will delete the SFX file to remove evidence of the file's existence. The backdoor will rename itself based on UID generated at start up, and subsequently, the file is moved

to **%LOCALAPPDATA%<uid>0.js** (e.g., 29e0d2550.js).

The backdoor creates a scheduled task to run with elevated permissions, as if initially executed by an admin user, and is used to maintain persistence on the system, and is named using the UID.

The backdoor looks for the file containing the keylogger**,** reads the contents, and decodes them using XOR operations. Decoded data is converted back into a hex string and stored in the Registry until ready to be executed. The data written to the Registry is a base64 encoded PowerShell command. The keylogger file is removed upon installation and the scheduled task is started to initiate immediate execution instead of waiting for a user to log on. The final installation task is to remove any volume shadow copies if the backdoor was running as admin to further clean up its tracks.

JavaScript backdoor and keylogger

Upon startup, and after the initial installation routine has been run, the backdoor will perform some preliminary steps before entering a loop where it will contact its C2 server and process any commands retrieved from the C2 server. The backdoor will look for any data contained in the configuration key **v,** which is used to store additional JavaScript code intended to be executed at startup.

The autostart JavaScript is not stored in **v** at installation and must be set later based on a C2 command. Next, the backdoor will attempt to start the keylogger stored as a base64 encoded PowerShell command retrieved and executed using a command via WMI. A keylogger component written in C# .Net is loaded by the JavaScript backdoor and runs concurrently with the backdoor. The source code for the keylogger is compiled and loaded into memory using a base64 encoded PowerShell command and creates a mutex to prevent multiple copies of the keylogger from running. The keylogger shares two of the configuration keys used by the backdoor to enable the two components to communicate and uses a configuration key to log captured keystrokes, which the backdoor sends to a C2; the keylogger does not have any network functionality.

Infrastructure

The DarkWatchman malware uses a domain generation algorithm (DGA) to generate a list of C2 domains that the malware attempts to communicate with different domains, potentially daily. The C2 URLs are created by combining the DGA domain list with the protocol, URL path, and a list of top-level domains (TLDs) that are hard coded in the backdoor. Previous TLDs included **.top**, **.fun**, **.online**, **.site,** whereas new TLDs include **.shop, .icu,** and **.cyou**. The backdoor creates and tests URLs starting with the original list, in which the DGA domains are added to, resulting in network connection attempts based on a static list of domains, then proceeding to the DGA domains.

System information is collected and generates a beacon:

- OS version/locale
- Domain role
- Computer name
- Username
- Current time zone
- Installed anti-virus
- Smartcard reader driver

Querying for the presence of a smartcard reader may indicate that Hive0117 conducts operations targeting military, government, or other organizations with higher security requirements.

MITRE ATT&CK alignment

T1027.010 Obfuscated Files or Information: Command Obfuscation

T1056.007 Command and Scripting Interpreter: JavaScript

T1053.005 Scheduled Task/Job: Scheduled Task

T1112 Modify Registry

Conclusion

A comparison of previously reported activity delivering DarkWatchman malware with the current activity, reveals a potential opportunist approach to operations featuring well-timed and manufactured campaigns. The fileless nature of the DarkWatchman malware, and its use of JavaScript and a keylogger written in C#, as well as the ability to remove traces of its existence on compromised systems when instructed, are evidence of somewhat sophisticated capabilities.

The ability of the malware to query for the presence of a smartcard reader may signal Hive0117's operational objectives including the compromise of military, government, or other organizations with elevated security requirements. X-Force recommends entities in-region remain at a heightened state of defensive security.

Recommendations

- Ensure anti-virus software and associated files are up to date.
- Search for existing signs of the indicated IoCs in your environment:
  - JS files in %LOCALAPPDATA% (e.g. 29e0d2550.js)
  - Supicious schedued taks (e.g., task name "29e0d255-29e0-d255-29e0-29e0d25529e0″)
  - Volume shadow copy deletion. Command: "vssadmin.exe Delete Shadows /All /Quiet"
  - Powershell commands launched from WMI. Command: "powershell.exe -NoP -NonI -W Hidden -Exec Bypass –enc <payload>"
  - Registry keys under"HKEY_CURRENT_USER\Software\Microsoft\Windows\DWM\<c_volume_serial>\
  - Registering dynwrapx.dll. Command: "regsvr32.exe /i /s %LOCALAPPDATA%\dynwrapx.dll"
- Consider blocking and/or setting up detection for all URLs matching the DGA format: [a-f0-9]{8}.[shop|icu|cyou|top|fun|online|site]/index.php
- Keep applications and operating systems running at the current released patch level.
- Exercise caution with attachments and links in emails.

To learn how IBM Security X-Force can help with anything regarding cybersecurity including incident response, threat intelligence or offensive security services, schedule a meeting here: IBM Security X-Force Scheduler.

If you are experiencing cybersecurity issues or an incident, contact IBM Security X-Force for help: US hotline 1-888-241-9812 | Global hotline (+001) 312-212-8034.

Indicators of compromise

Indicator	Indicator Type	Context
03735369a2e4a40528076f8e2f1e1501056fbc7bb70a2d30e364c3e17e670917	Email ZIP Attachment	Мобилизационное предписание №291-76005-23 от 10.05.2023.zip
e35f82f85a608553483482ce7297d49de205f609961d8bf3511cb1a00bcad956	Email ZIP Attachment	Мобилизационное предписание №5010421409-ВВК от 10.05.2023.zip

Indicator	Indicator Type	Context
3aa2a15dabbf0f5a18232b7f849c9d340bf27e4048a65c80c4519f97f44e6e87	ZIP File	Мобилизационное предписание №314-39008-3Н от 10.05.2023.zip
183c4d8170e7ca73992f05d336f7b1e3cfc4d6b4f28be585ee37d7d2085305a9	ZIP File	Мобилизационное предписание №4212317-009МК от 10.05.2023.zip
540b6af8474a9725dd44fb493263a91b43409af34899eb77349120503135fc73	ZIP File	Мобилизационное предписание №186-31005-23 от 10.05.2023.zip
de8c0e985eb2426668c4b72c925cdd4d28b9d3018177949c4d69557b718c0fea	Javascript	c784477d0.js
0b7da98101170c42365b0cf2ae2b1b86c5ea035731e46a951fd729fb7bb7a019	Javascript	c784477d0.js
f103d0043f1246818615c34c863f985b89fceb4baa1d7ad724ec505bf7dcc165	Javascript	c153ea2b0.js
c03a9409f79d8766bf70719ef6c97db5de72527d9daf634e8e65d912d42da20d	Javascript	36d1130a0.js
99cdd88c12687b383af72aa6401808c447994489f2d2b45521dc673b03f24a21	Javascript	d46026150.js
7860768264fdf663ff3b78e0efffd427cfe56be82ce32214f550d6103205c922	EXE	Заявка_05062023.exe
4413d38812f17ed73bfb67854415038fd9e2e246ccbdaf64f178abf2aee06e27	EXE	Заявка_05062023.exe
483fcdd6983631f27ca31a55cfd5cc41c0800a3ac4d4ce5e10f8a1664bb15c11	EXE	dogovor.exe
69fa6b29f2b7954675949cdca29eda7d00f36e8f6bfde2a43efa422ab7d545d5	EXE	
c19e0be9400279b5aee97862435802934419e0ff116a78b292565bd5edc5d446	EXE	Заявка_05062023.exe
d439a3ce7353ef96cf3556abba1e5da77eac21fdba09d6a4aad42d1fc88c1e3c	EXE	
dcf8c16ea3b02a94e22709b4449a174a59545bf31a64627fee144b67733888dc	EXE	Заявка_05062023.exe
mail[@]voenkomat-mil[.]ru	Email Address	Return Path
025ad916.cyou	Domain	C2
025ad916.icu	Domain	C2
025ad916.shop	Domain	C2
ec311447.cyo	Domain	C2
ec311447.shop	Domain	C2
ec311447.icu	Domain	C2
9da3ecce.cyou	Domain	C2
9da3ecce.icu	Domain	C2
9da3ecce.shop	Domain	C2
1ee79f0e.cyou	Domain	C2

Indicator	Indicator Type	Context
1ee79f0e.shop	Domain	C2
1ee79f0e.icu	Domain	C2
0f580158.cyou	Domain	C2
0f580158.shop	Domain	C2
0f580158.icu	Domain	C2

Scroll to view full table

IBM X-Force Research | Malware Analysis | Phishing | Phishing Email | X-Force

Claire Zaboeva
Senior Strategic Cyber Threat Analyst, IBM

Melissa Frydrych
Threat Hunt Researcher, IBM

Golo Mühr
X-Force Threat Intelligence, IBM