



## **| Profile |**

# **APT28 Distributes New Malware Strains: OCEANMAP, MASEPIE, and STEELHOOK**

**P-2024-01-09a**

**Classification: TLP:CLEAR**

**Criticality: High**

**Intelligence Requirements: Vulnerability Exploitation, Malware, Deep Dark Web & Criminal Underground**

**January 9, 2024**



## **Profile**

### **APT28 Distributes New Malware Strains: OCEANMAP, MASEPIE, and STEELHOOK**

**Created on:** January 8, 2024

**Intelligence Cut-off:** 01:00 PM (EST) on  
January 4, 2024

|                            |                          |
|----------------------------|--------------------------|
| <b>First Observed</b>      | <b>December 15, 2023</b> |
| <b>Origin</b>              | <b>APT 28 (Russia)</b>   |
| <b>Motivation</b>          | <b>Cyber Espionage</b>   |
| <b>Targeted Industries</b> | <b>Government</b>        |
| <b>Targeted Nations</b>    | <b>Ukraine, Poland</b>   |

## **New Campaign Detected**

On December 28, 2023, the Computer Emergency Response Team of Ukraine (CERT-UA) released an advisory on a new phishing campaign by Russia state-affiliated Advanced Persistent Threat (APT) group APT28 (aka Fancy Bear, Sednit, Pawn Storm, and Sofacy Group). Detected between December 15 and December 25, the campaign utilizes previously undocumented malware strains—namely, OCEANMAP, MASEPIE, and STEELHOOK—to collect information from the networks of numerous Ukrainian government entities, as well as possibly several undisclosed Polish organizations.<sup>12</sup> The extent of the sensitive information stolen in these attacks has not yet been publicly disclosed.

<sup>1</sup> [hXXps://cert\[.\]gov\[.\]ua/article/6276894](https://cert.gov.ua/article/6276894)

<sup>2</sup> [hXXps://thehackernews\[.\]com/2023/12/cert-ua-uncovers-new-malware-wave.html](https://thehackernews[.]com/2023/12/cert-ua-uncovers-new-malware-wave.html)

# **Profile | APT28 Distributes New Malware Strains: OCEANMAP, MASEPIE, and STEELHOOK**

P-2024-01-08a  
TLP: CLEAR



The attack commences with the distribution of phishing emails to employees of the target entities containing a link to view a document. The link redirects the victim to a compromised web resource that exploits the “search” / “search-ms” Uniform Resource Identifier (URI) protocol handler via JavaScript to download a shortcut file (LNK). Once opened, the file launches PowerShell commands to then activate the Server Message Block (SMB) Protocol, allowing for the download of a decoy document from a remote server, the Python programming language interpreter, and a Client.py file now categorized as MASEPIE.<sup>345</sup>

- MASEPIE is a malicious backdoor developed in Python that is used to upload and download files, as well as execute commands, utilizing the Transmission Control Protocol (TCP) as the communications channel to the command-and-control (C2) server. Using MASEPIE, APT28 actors then execute additional malware strains—predominantly OCEANMAP and STEELHOOK.<sup>6</sup>
- OCEANMAP is a malicious backdoor developed in the C# programming language that is used to execute commands using cmd.exe. It utilizes the Internet Message Access Protocol (IMAP) as the communications channel to the C2 server.<sup>7</sup>
- STEELHOOK is a PowerShell script that allows for the theft of Chrome and Edge browser data, as well as the Data Protection Application Programming Interface (DPAPI) master key used for encryption and decryption purposes.<sup>89</sup>
- In addition to the three aforementioned malware strains, APT28 actors also execute OPENSSH to build a network tunnel and exploit IMPACKET and SMBEXEC to attempt to move laterally.<sup>10</sup>

---

<sup>3</sup> [hXXps://cert\[.\]gov\[.\]ua/article/6276894](https://cert[.]gov[.]ua/article/6276894)

<sup>4</sup> [hXXps://thehackernews\[.\]com/2023/12/cert-ua-uncovers-new-malware-wave.html](https://thehackernews[.]com/2023/12/cert-ua-uncovers-new-malware-wave.html)

<sup>5</sup> [hXXps://securityaffairs\[.\]com/156623/apt/apt28-phishing-new-malware.html](https://securityaffairs[.]com/156623/apt/apt28-phishing-new-malware.html)

<sup>6</sup> [hXXps://cert\[.\]gov\[.\]ua/article/6276894](https://cert[.]gov[.]ua/article/6276894)

<sup>7</sup> *Ibid.*

<sup>8</sup> *Ibid.*

<sup>9</sup> [hXXps://securityaffairs\[.\]com/156623/apt/apt28-phishing-new-malware.html](https://securityaffairs[.]com/156623/apt/apt28-phishing-new-malware.html)

<sup>10</sup> [hXXps://cert\[.\]gov\[.\]ua/article/6276894](https://cert[.]gov[.]ua/article/6276894)

# Profile | APT28 Distributes New Malware Strains: OCEANMAP, MASEPIE, and STEELHOOK

P-2024-01-08a  
TLP:CLEAR



## MASEPIE, OCEANMAP, and STEELHOOK Attack Overview

Source: [hXXps://thehackernews\[.\]com/2023/12/cert-ua-uncovers-new-malware-wave.html](https://thehackernews.com/2023/12/cert-ua-uncovers-new-malware-wave.html)

## APT28 Background

Active since at least 2004, APT28 is a cyber espionage group operating under the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (formerly the Main Intelligence Directorate and still commonly known by its previous abbreviation, GRU). The group has an extensive and successful history of targeting government, military, and security entities across the globe utilizing sophisticated techniques, and procedures (TTPs) similar to the phishing and advanced malware deployment techniques seen in these latest attacks.<sup>1112</sup> APT28 has targeted high-profile entities in the past, such as the U.S. Democratic National Committee in 2016, and is also known to utilize current geopolitical topics as lures to deploy the custom backdoor HeadLace, as seen in recent attacks capitalizing on the Israel-Hamas War. The group has also exploited an Outlook email vulnerability (CVE-2023-23397), predominantly to target Polish nationals.<sup>1314</sup> Each APT28 attack typically results in a high payout for the group; ZeroFox

<sup>11</sup> [hXXps://www.secureworks\[.\]com/research/threat-profiles/iron-twilight](https://www.secureworks.com/research/threat-profiles/iron-twilight)

<sup>12</sup> [hXXps://www.radware\[.\]com/cyberpedia/ddos-attacks/fancy-bear-apt28-threat-actor/](https://www.radware.com/cyberpedia/ddos-attacks/fancy-bear-apt28-threat-actor/)

<sup>13</sup> [hXXps://thehackernews\[.\]com/2023/12/russian-apt28-hackers-targeting-13.html](https://thehackernews.com/2023/12/russian-apt28-hackers-targeting-13.html)

<sup>14</sup> [hXXps://thehackernews\[.\]com/2023/12/microsoft-warns-of-kremlin-backed-apt28.html](https://thehackernews.com/2023/12/microsoft-warns-of-kremlin-backed-apt28.html)

# **Profile | APT28 Distributes New Malware Strains: OCEANMAP, MASEPIE, and STEELHOOK**

P-2024-01-08a  
TLP: CLEAR



assesses with moderate confidence that these latest attacks using the novel OCEANMAP, MASEPIE, and STEELHOOK malware strains are likely no exception.

## **Recommendations**

To mitigate the risk of network compromise due to these novel malware strains, organizations should:

- Conduct heightened social engineering awareness and training for relevant stakeholders.
- Use a layered security framework to ensure all malicious emails and attachments are properly identified and blocked.
- Consider implementing a segmented network in order to impede compromise of the entire network.
- Utilize the ZeroFox Platform to perform searches on relevant Indicators of Compromise (IOCs) and monitor for further developments.

## **| Appendix A: IOCs**

### **Files Names**

- 2.txt
- 2.ps1 (**STEELHOOK**)
- VMSearch.sfx.exe
- Client.py (**MASEPIE**)
- VMSearch.exe (**OCEANMAP**)
- KFP.311.152.2023.pdf.Ink
- Strategies of Ukraine.pdf.Ink

### **File Hashes - MD5**

- 9724cecaa8ca38041ee9f2a42cc5a297
- 5f126b2279648d849e622e4be910b96c
- 47f4b4d8f95a7e842691120c66309d5b
- 8d1b91e8fb68e227f1933cfab99218a4
- 6fdd416a768d04a1af1f28ecaa29191b
- 5db75e816b4cef5cc457f0c9e3fc4100
- 6128d9bf34978d2dc7c0a2d463d1bcdd
- 825a12e2377dd694bbb667f862d60c43
- Acd9fc44001da67f1a3592850ec09cb7

### **File Hashes - SHA-256**

- 4fa8caea8002cd2247c2d5fd15d4e76762a0f0cdb7a3c9de5b7f4d6b2ab34ec6
- 6bae493b244a94fd3b268ff0feb1cd1fbc7860ecf71b1053bf43eea88e578be9
- 18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6
- 6d44532b1157ddc2elf41df178ea9cbc896c19f79e78b3014073af2d8d9504fe
- Fb2c0355b5c3adc9636551b3fd9a861f4b253a212507df0e346287110233dc23
- 24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04
- 19d0c55ac466e4188c4370e204808ca0bc02bba480ec641da8190cb8aee92bdc
- 593583b312bf48b7748f4372e6f4a560fd38e969399cf2a96798e2594a517bf4
- c22868930c02f2d6962167198fde0d3cda78ac18af506b57f1ca25ca5c39c50d

### **Network**

- \\194.126.178[.]8@80\webdav\Docs\231130 No. 581.pdf .Ink
- \\194.126.178[.]8@80\webdav\Docs\231130 No. 581.pdf

# **Profile | APT28 Distributes New Malware Strains: OCEANMAP, MASEPIE, and STEELHOOK**

P-2024-01-08a  
TLP: CLEAR



- \\194.126.178[.]8@80\webdav\Python39\Client.py
- \\194.126.178[.]8@80\webdav\Python39\python.exe
- 173.239.196[.]66 (**X-Originating-IP**)
- (tcp)://88.209.251[.]6:80
- 194.126.178[.]8
- 88.209.251[.]6
- 74.124.219[.]71 (**OCEANMAP C2**)
- czyrqdnvpujmmjkfhhs4knflav02demj.oast[.]fun
- czyrqdnvpujmmjkfhhsclx05sfi23bfr.oast[.]fun
- czyrqdnvpujmmjkfhhs gapqr3hclnhhj.oast[.]fun
- czyrqdnvpujmmjkfhhsvlaax17vd5r6v.oast[.]fun
- hXXp://194.126.178[.]8/webdav/wody.pdf
- hXXp://194.126.178[.]8/webdav/wody.zip
- hXXp://194.126.178[.]8/webdav/StrategyUa.pdf
- hXXp://194.126.178[.]8/webdav/231130N581.pdf
- hXXp://czyrqdnvpujmmjkfhhsclx05sfi23bfr.oast[.]fun
- hXXp://czyrqdnvpujmmjkfhhs gapqr3hclnhhj.oast[.]fun
- hXXp://czyrqdnvpujmmjkfhhsvlaax17vd5r6v.oast[.]fun
- hXXp://czyrqdnvpujmmjkfhhs4knflav02demj.oast[.]fun
- hXXps://nas-files.firstcloudit[.]com/
- hXXps://ua-calendar.firstcloudit[.]com/
- hXXps://e-nas.firstcloudit[.]com/
- jrb@bahouholdings[.]com (**OCEANMAP C2**)
- nas-files.firstcloudit[.]com
- e-nas.firstcloudit[.]com
- ua-calendar.firstcloudit[.]com
- qasim.m@facadesolutionsuae[.]com (**OCEANMAP C2**)
- webmail.facadesolutionsuae[.]com (**OCEANMAP C2**)

## **| Appendix B: Traffic Light Protocol for Information Dissemination**

### **WHEN SHOULD IT BE USED?**

#### **Red**

##### **Sources may use**

**TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

#### **Amber**

##### **Sources may use**

**TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

### **HOW MAY IT BE SHARED?**

##### **Recipients may NOT share**

**TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

##### **Recipients may ONLY share**

**TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

##### **Note that**

**TLP:AMBER+STRICT** restricts sharing to the organization only.

#### **Green**

### **WHEN SHOULD IT BE USED?**

##### **Sources may use**

**TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

#### **Clear**

##### **Sources may use**

**TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

### **HOW MAY IT BE SHARED?**

##### **Recipients may share**

**TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.

##### **Recipients may share**

**TLP:CLEAR** information without restriction, subject to copyright controls.

## Appendix C: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

| Almost No Chance | Very Unlikely | Unlikely | Roughly Even Chance | Likely | Very Likely | Almost Certain |
|------------------|---------------|----------|---------------------|--------|-------------|----------------|
| 1-5%             | 5-20%         | 20-45%   | 45-55%              | 55-80% | 80-95%      | 95-99%         |