
Cyber Threat Advisory

Fighting Ursa
Threat Actor Malware

Description

Fighting Ursa

Fighting Ursa, also known as APT28, Fancy Bear, and Sofacy, is a Russian state-sponsored advanced persistent threat (APT) group. It can affect United States, United Kingdom, Germany, France, Ukraine, Russia and Asia .They are highly skilled and persistent, known for their use of spear phishing, malware, and other cyberespionage techniques to target government organizations, media outlets, and political entities. Their operations often aim to steal sensitive information, conduct surveillance, and disrupt critical infrastructure.

CATEGORY

Malware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- Economic Espionage
- Financial Loss
- Damage to International Relations
- Espionage and Intelligence Gathering

Indicator of compromise

SHA-256

```
cda936ecae566ab871e5c0303d8ff98796b1e3661885afd9d4690fc1e945640e  
7c85ff89b535a39d47756dfce4597c239ee16df88badefe8f76051b836a7cbfb  
dad1a8869c950c2d1d322c8aed3757d3988ef4f06ba230b329c8d510d8d9a027  
c6a91cba00bf87cdb064c49adaac82255cbec6fdd48fd21f9b3b96abf019916b  
6b96b991e33240e5c2091d092079a440fa1bef9b5aecbf3039bf7c47223bdf96  
a06d74322a8761ec8e6f28d134f2a89c7ba611d920d080a3ccbfa7c3b61e2e7
```

SHA-1

```
010e1bdb8129ee16bf9803a75038d7a3add28939  
ace64c642bbab201acea3ea8b85277b678358c8a  
04dbf45f86d3643b9565ce54f4b8d6307de3975  
42d36eeb2140441b48287b7cd30b38105986d68f  
590c431b7a7b16bd731ab660f611ed54e8dc1bb0  
cdb5e213c55f1c631eb5c58c46a80734dac74ae3
```

| MD-5

849129c405369cb5e61d3f509655db6f
ed3619f4415eba888dc20c2adf679a4a
479252c7a08cb0b14defa95e2d26c14e
10e4a1d2132ccb5c6759f038cdb6f3c9
e3604d4fa956025486bce7da25296cd9
15f56bd7b1f78912ef38b36ff3ab8a49

| Remediation

- **Employee Training:** Regular cybersecurity awareness training is crucial to prevent phishing and social engineering attacks.
- **Patch Management:** Keep operating systems, applications, and software up-to-date with the latest patches to address vulnerabilities.
- **Access Controls:** Implement robust access controls, including strong password policies, multi-factor authentication (MFA), and role-based access controls.
- **Network Segmentation:** Isolate critical systems and networks to limit the impact of a potential breach.
- **Data Backup and Recovery:** Regular backups and a robust disaster recovery plan are essential to protect data integrity.
- **Endpoint Protection:** Deploy robust endpoint protection solutions with advanced threat detection capabilities.
- **Email Security:** Utilize email security solutions to filter spam, phishing attacks, and malicious attachments.
- **Block all IOCs on your XDR, EDR and other security tools.**

Cyber Threat Advisory

Secure your byte world



+1 (832) 271 2738



info@threatcure.net



<https://threatcure.net/>