THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

FancyBear APT28

Threat Actor Criminal

CATEGORY

Criminal

SEVERITY

High

Platforms

Windows, MacOS, Linux

IMPACT

- Unauthorized Access to Information
- Extraction of Confidential Data
- Disclosure of Critical Details

Description

FancyBear APT28

APT28, one of Russia's most persistent advanced persistent threat (APT) groups, has been active since at least 2007. The group targets entities in the U.S., Europe, Asia, and former Soviet states to advance Russia's strategic goals. Actively operating in Asia, APT28 focuses on cyberattacks against military, defense, and financial institutions, aiming to disrupt operations, exfiltrate sensitive data, and leak information to Russian authorities. Known by aliases such as Fancy Bear, Pawn Storm, and Sofacy Group, the group employs phishing emails with malicious links and spoofed websites to infiltrate systems. In February 2022, APT28 allegedly targeted Eastern Europe using tools like Empire and Invoke-Obfuscation while exploiting the MSHTML Remote Code Execution vulnerability (CVE-2021-40444).

Recent campaigns have focused on Polish organizations, utilizing JavaScript and "ms-search" mechanisms to deploy malware, including MASEPIE, STEELHOOK, OCEAN MAP, and OpenSSH. APT28 frequently uses PowerShell scripts to conduct reconnaissance, lateral movement, and data exfiltration. By leveraging PowerShell's integration with the Windows operating system, attackers exploit its functionality and privileges to execute malicious activities with precision and efficiency.

Indicator of Compromise

SHA256

```
ad1a495282bb10362b9244993c2f6ef63d19359251f07eb5edea9787cb064c06
ed6a6e1bfacaa0d18f44616342463cc6702a80d24ea1b7750f0b4305dade2673
d69fa80c8e54e8331e63c2d130a5d7b475f8c378971d9571db1d368662f7d6fd
82bfcdb70be97eabfe30ffcbe53b0b3cbafb352698f4a7cd590223f32aa10aec
c50bdb7b4732bef5aa7dc8b392bf95e69cd01e81e6e4a0d4b6d90c541a2929c5
e9711f47cf9171f79bf34b342279f6fd9275c8ae65f3eb2c6ebb0b8432ea14f8
6ebc89d9262d38efb4f2d72b0a55cb60d228cf1a71b026a261fe4768131beecb
2f694f5b72b4da3f9c6c674003ed36f5591a997ad5bde817d0fdc3f1c4792956
37d7f927abcd4d1bf617e8279b8b8d7c8b14abec089e856faa6ffe36937c4e16
e8ad660d43a15987b493debd58a0107f0fa62857d9930806873028fb0475df0b
```

Indicator of Compromise

MD5

4495b2812d6b35fd8d1c130531151a16
4a2db38af38cd2b3bb1836643cd5b731
536998185193b231e62d404c51121b8c
88685ceb4e3b78169a3c8f8b18d98f2a
21094565a757b9b979fb62c5d2a311b4
e06b24113cab27ff5a1173fa3f9e1615
9bfc3e89c54cb23a7afe61778b4498a1
bd4eb7a629dc716c4884ba77b338b00f
ef4579d6e1e665056bc593ecbad1e473
a60f3a96bfa741a606f493182e2f146a

Remediation

- Restrict all identified threat indicators using your security tools.
- Use security controls to search for Indicators of Compromise (IOCs) within your network.
- Apply robust security measures such as enforcing strong passwords, maintaining accurate configurations, and adhering to effective administrative policies.
- Handle emails from unfamiliar sources with caution.
- Avoid clicking on links or opening attachments from unknown senders.

ThreatCure

Cyber Threat Advisory

Secure your byte world

FancyBear APT28

Threat Actor Criminal

Get Started Today

For more information about the ThreatCure ShieldOps Platform
or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE