Dec 07 2023

NETMANAGEIT

Intelligence Report

Fighting Ursa Aka APT28: Illuminating a Covert Campaign

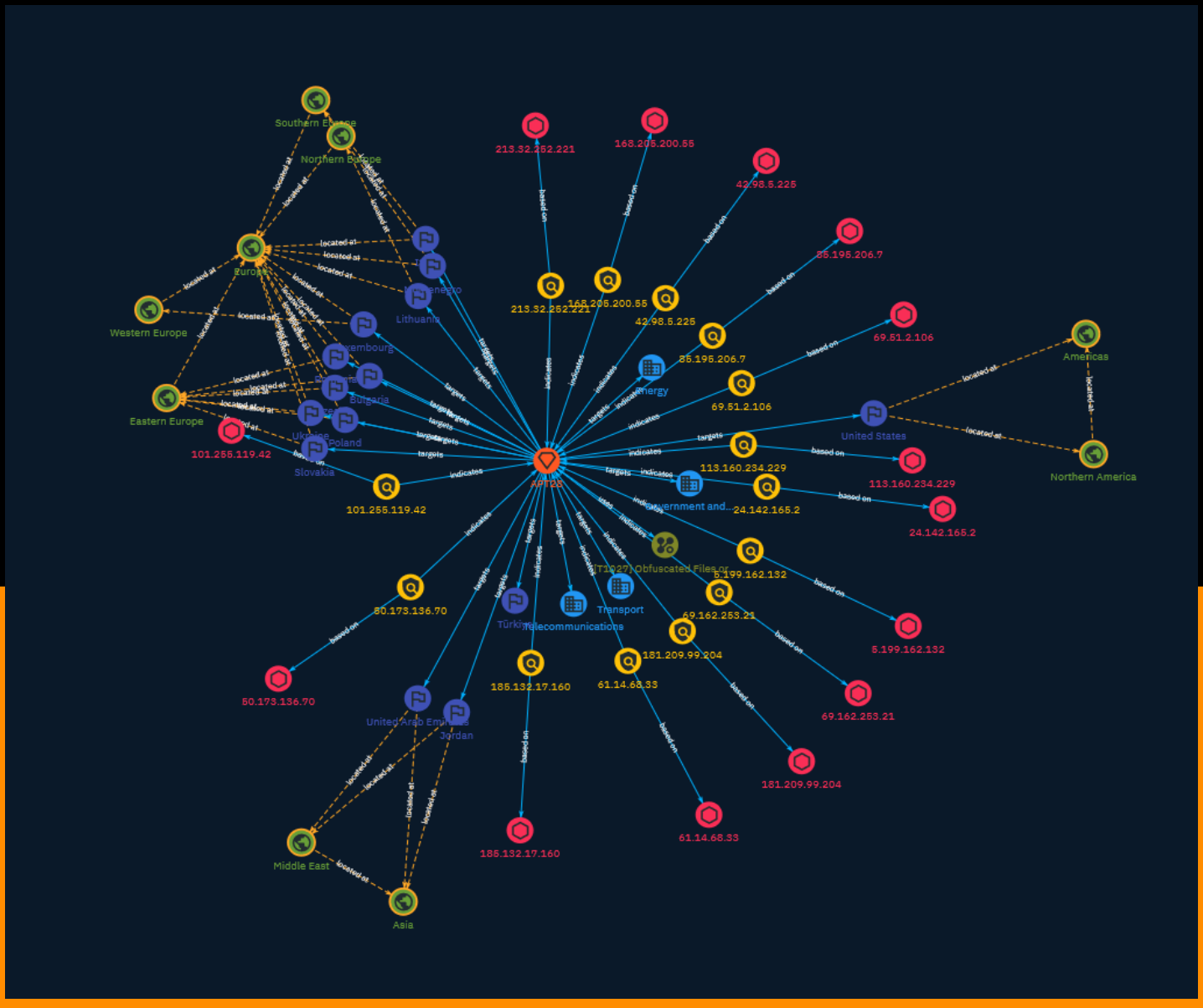

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Early this year, Ukrainian cybersecurity researchers found Fighting Ursa leveraging a zero-day exploit in Microsoft Outlook (now known as CVE-2023-23397). This vulnerability is especially concerning since it doesn't require user interaction to exploit. Unit 42 researchers have observed this group using CVE-2023-23397 over the past 20 months to target at least 30 organizations within 14 nations that are of likely strategic intelligence value to the Russian government and its military.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Obfuscated Files or Information
ID
T1027
Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Sector

Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.
Name
Transport
Description
All entities involved in the movement of people or goods from one place to another.
Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Indicator

Name
213.32.252.221
Description
TrickBot botnet C2 server (confidence level: 75%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '213.32.252.221']
Name
85.195.206.7
Description
CC=CH ASN=AS13030 Init7 (Switzerland) Ltd.
Pattern Type
stix

Pattern

[ipv4-addr:value = '85.195.206.7']

Name

61.14.68.33

Description

CC=SG ASN=AS134078 NETPLUZ HOLDINGS PRIVATE LIMITED

Pattern Type

stix

Pattern

[ipv4-addr:value = '61.14.68.33']

Name

50.173.136.70

Description

Responder botnet C2 server (confidence level: 50%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.173.136.70']

Name

181.209.99.204

Description

ISP: ARSAT - Empresa Argentina de Soluciones Satelitales S.A. **OS:** None ---------- Hostnames: - 204.99.209.181.in-addr.arpa ---------- Domains: - 181.in-addr.arpa ---------- Services: **22:** ``` SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCY+9SA+ZTqlvXaXCyihhByuBlHSvcrwB46QEqtazX/K8c63Vfe0x1/fIL6YHUR2vtl8/wKxvkok85pNc/Jg1u5pKU39av27cmSOc2TJvxkD+75Oqcer3/JgFn3 /vspyWWvPAVyxMskPlMaFfYZNVQFdQSUTsuz0GIBlf7D/cUbWP+Djb1uBsjPaR49GUSgM1pkdEPXQg3oJKEqW03qjd+CPBz3C/hRL3QtXpqzb55q0ioc/7XilP0YJ9az+LDbKQrBycAoVqI8Lg2kzBlJz+FJHrZvE077igW/yZnUqDfBjszRNqcUAiVwOZdt4V7cM0VtrXU75jXsZ3dF7WkZrYaB Fingerprint: f7:05:60:b3:85:57:5f:d5:3e:b4:31:42:69:6c:70:c3 Kex Algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ssh-dss ecdsa-sha2-nistp256 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-cbc 3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5 hmac-sha1 umac-64@openssh.com hmac-sha2-256 hmac-sha2-256-96 hmac-sha2-512 hmac-sha2-512-96 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ``` ---------- **123:** ``` NTP protocolversion: 3 stratum: 3 leap: 0 precision: -14 rootdelay: 0.152725219727 rootdisp: 0.123123168945 refid: 2824928195 reftime: 3910234747.17 poll: 3 ``` ---------- **500:** ``` VPN (IKE) Initiator SPI: 316f6e77797a6662 Responder SPI: 7335726f33373278 Next Payload: RESERVED Version: 2.0 Exchange Type: DOI Specific Use Flags: Encryption: False Commit: False Authentication: False Message ID: 00000000 Length: 36 ``` ---------- **1701:** ``` \xc8\x02\x00\x0c\x00\x00\x00\x00\x00\x00\x01 ``` ---------- **1723:** ``` PPTP: Firmware: 1 Hostname: local Vendor: linux ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '181.209.99.204']

Name
185.132.17.160
Description
CC=CH ASN=AS21232 Genossenschaft GGA Maur
Pattern Type
stix
Pattern
[ipv4-addr:value = '185.132.17.160']
Name
42.98.5.225
Description
CC=HK ASN=AS4760 HKT Limited
Pattern Type
stix
Pattern
[ipv4-addr:value = '42.98.5.225']
Name
5.199.162.132

Description

CC=LT ASN=AS16125 UAB Cherry Servers

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.199.162.132']

Name

101.255.119.42

Description

ISP: PT Remala Abadi **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **123:** ``` NTP protocolversion: 3 stratum: 3 leap: 0 precision: -15 rootdelay: 0.128433227539 rootdisp: 0.0734558105469 refid: 1729213982 reftime: 3910910688.32 poll: 3 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '101.255.119.42']

Name

69.162.253.21

Description
CC=US ASN=AS53407 UTOPIA-FIBER
Pattern Type
stix
Pattern
[ipv4-addr:value = '69.162.253.21']
Name
24.142.165.2
Description
CC=US ASN=AS10796 TWC-10796-MIDWEST
Pattern Type
stix
Pattern
[ipv4-addr:value = '24.142.165.2']
Name
113.160.234.229
Description

ISP: VNPT Corp **OS:** None ------------------------- Hostnames: - static.vnpt.vn ------------------------- Domains: - vnpt.vn ------------------------- Services: **80:** ``` HTTP/1.1 302 Found Date: Wed, 06 Dec 2023 04:20:11 GMT X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' X-XSS-Protection: 1; mode=block Location: https://113.160.234.229:443/ Content-Length: 212 Content-Type: text/html; charset=iso-8859-1 ``` ------------------ **443:** ``` HTTP/1.1 404 Not Found Date: Wed, 06 Dec 2023 15:20:58 GMT X-Frame-Options: SAMEORIGIN Content-Security-Policy: frame-ancestors 'self' X-XSS-Protection: 1; mode=block Strict-Transport-Security: max-age=15552000 Content-Length: 123 ``` HEARTBLEED: 2023/12/06 15:21:15 113.160.234.229:443 - SAFE ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '113.160.234.229']

Name

69.51.2.106

Description

ISP: Elite Broadband LLC **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **80:** ``` HTTP/1.1 301 Moved Permanently Location: https://69.51.2.106:443/ Content-Length: 0 Date: Sat, 02 Dec 2023 03:57:49 GMT Server: Server ``` ------------------ **123:** ``` NTP protocolversion: 3 stratum: 3 leap: 0 precision: -14 rootdelay: 0.0735473632812 rootdisp: 0.0275421142578 refid: 3233628603 reftime: 3909554868.14 poll: 3 ``` ------------------ **443:** ``` ``` ------------------ **2222:** ``` SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDx0Jjq89iDjazn4baYaENrC6DP/zw1M3T+apQ8DRm53A+W VZ/hxe1c/1iyicjqVasbr3woU4qBRedciJJW+TaZ42Nac2gKVzGeLaD5GkbMxOYdUSHmeY8io/mmKbM4Pyygfkbz0ILKqixDBla7mDLOYLpNd5I1QgHkbYwn/IuGkcJgsYU/BJZuW8jPrh7nMDhB1AK0bPOB2PhT3XfUCMDNbbAapV079mHi0JYf5kl5Y78kvDeEfMyDOR99oeGKdljD9b59x4c+tu6oHy4eml6vWG0HbDuY9OVbu6L62FQS0KQhIs3y0C0MlqVrmnH0RiKX2eTmkz0u+ZWNuSUk7Q8T Fingerprint: c5:e4:66:fb:4f:51:e3:3e:db:fc:99:99:48:34:79:d0 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '69.51.2.106']

Name

168.205.200.55

Description

ISP: BR INTERNET LDTA-ME **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **5060:** ``` SIP/2.0 200 OK Via: SIP/2.0/UDP nm;branch=foo;rport=26810;received=224.52.252.100 From: ;tag=root To: ;tag=1917058449 Call-ID: 50000 CSeq: 42 OPTIONS Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, SUBSCRIBE, NOTIFY, INFO, UPDATE Accept: application/sdp User-Agent: Comnect Sip Agent/3.6.0 Allow-Events: dialog, message-summary, refer, reg, ua-profile Content-Length: 0 ``` ---------- **8081:** ``` HTTP/1.0 302 Moved Temporarily Date: Thu, 07 Dec 2023 03:43:46 GMT Server: Boa/0.93.15 Connection: close Content-Type: text/html Location: /admin/login.asp

302 Moved

The document has moved here. ``` ----------

Pattern Type
stix

Pattern
[ipv4-addr:value = '168.205.200.55']

Intrusion-Set

Name

APT28

Description

[APT28](https://attack.mitre.org/groups/G0007) is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.(Citation: NSA/FBI Drovorub August 2020)(Citation: Cybersecurity Advisory GRU Brute Force Campaign July 2021) This group has been active since at least 2004.(Citation: DOJ GRU Indictment Jul 2018)(Citation: Ars Technica GRU indictment Jul 2018)(Citation: Crowdstrike DNC June 2016)(Citation: FireEye APT28)(Citation: SecureWorks TG-4127)(Citation: FireEye APT28 January 2017)(Citation: GRIZZLY STEPPE JAR)(Citation: Sofacy DealersChoice)(Citation: Palo Alto Sofacy 06-2018)(Citation: Symantec APT28 Oct 2018)(Citation: ESET Zebrocy May 2019) [APT28](https://attack.mitre.org/groups/G0007) reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. (Citation: Crowdstrike DNC June 2016) In 2018, the US indicted five GRU Unit 26165 officers associated with [APT28](https://attack.mitre.org/groups/G0007) for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations.(Citation: US District Court Indictment GRU Oct 2018) Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as [Sandworm Team](https://attack.mitre.org/groups/G0034).

Country

Name
Czechia
Name
Slovakia
Name
United Arab Emirates
Name
Poland
Name
Luxembourg
Name
Bulgaria
Name
Lithuania

Name
United States
Name
Türkiye
Name
Italy
Name
Jordan
Name
Romania
Name
Montenegro
Name
Ukraine

Region

Name
Europe
Name
Northern Europe
Name
Asia
Name
Southern Europe
Name
Northern America
Name
Eastern Europe
Name
Western Europe

Name
Middle East

Name
Americas

IPv4-Addr

Value
101.255.119.42
5.199.162.132
185.132.17.160
168.205.200.55
61.14.68.33
50.173.136.70
85.195.206.7
69.162.253.21
24.142.165.2
113.160.234.229
69.51.2.106
42.98.5.225
181.209.99.204

213.32.252.221

External References

- https://otx.alienvault.com/pulse/6572250f298d2a69b238cf72
- https://unit42.paloaltonetworks.com/russian-apt-fighting-ursa-exploits-cve-2023-233397/