National Security Agency
Cybersecurity & Infrastructure Security Agency
Federal Bureau of Investigation
National Cyber Security Centre a part of GCHQ
Cybersecurity Advisory

Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments

Executive summary

Since at least mid-2019 through early 2021, Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165, used a Kubernetes® cluster to conduct widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide. GTsSS malicious cyber activity has previously been attributed by the private sector using the names Fancy Bear, APT28, Strontium, and a variety of other identifiers. The 85th GTsSS directed a significant amount of this activity at organizations using Microsoft Office 365® cloud services; however, they also targeted other service providers and on-premises email servers using a variety of different protocols. These efforts are almost certainly still ongoing.

This brute force capability allows the 85th GTsSS actors to access protected data, including email, and identify valid account credentials. Those credentials may then be used for a variety of purposes, including initial access, persistence, privilege escalation, and defense evasion. The actors have used identified account credentials in conjunction with exploiting publicly known vulnerabilities, such as exploiting Microsoft Exchange servers using CVE 2020-0688 and CVE 2020-17144, for remote code execution and further access to target networks. After gaining remote access, many well-known tactics, techniques, and procedures (TTPs) are combined to move laterally, evade defenses, and collect additional information within target networks.

Network managers should adopt and expand usage of multi-factor authentication to help counter the effectiveness of this capability. Additional mitigations to ensure strong access controls include time-out and lock-out features, the mandatory use of strong passwords, implementation of a Zero Trust security model that uses additional attributes when determining access, and analytics to detect anomalous accesses. Additionally, organizations can consider denying all inbound activity from known anonymization services, such as commercial virtual private networks (VPNs) and The Onion Router (TOR), where such access is not associated with typical use.

Description of targets

This campaign has already targeted hundreds of U.S. and foreign organizations worldwide, including U.S. government and Department of Defense entities. While the sum of the targeting is global in nature, the capability has predominantly focused on entities in the U.S. and Europe. Types of targeted organizations include:

Government and military organizations[1]

Political consultants and party organizations[2]

Defense contractors

Energy companies

Logistics companies

Think tanks

Higher education institutions

Law firms

Media companies

Known TTPs

The actors used a combination of known TTPs in addition to their password spray operations to exploit target networks, access additional credentials, move laterally, and collect, stage, and exfiltrate data, as illustrated in the figure below. The actors used a variety of protocols, including HTTP(S), IMAP(S), POP3, and NTLM. The actors also utilized different combinations of defense evasion TTPs in an attempt to disguise some components of their operations; however, many detection opportunities remain viable to identify the malicious activity.

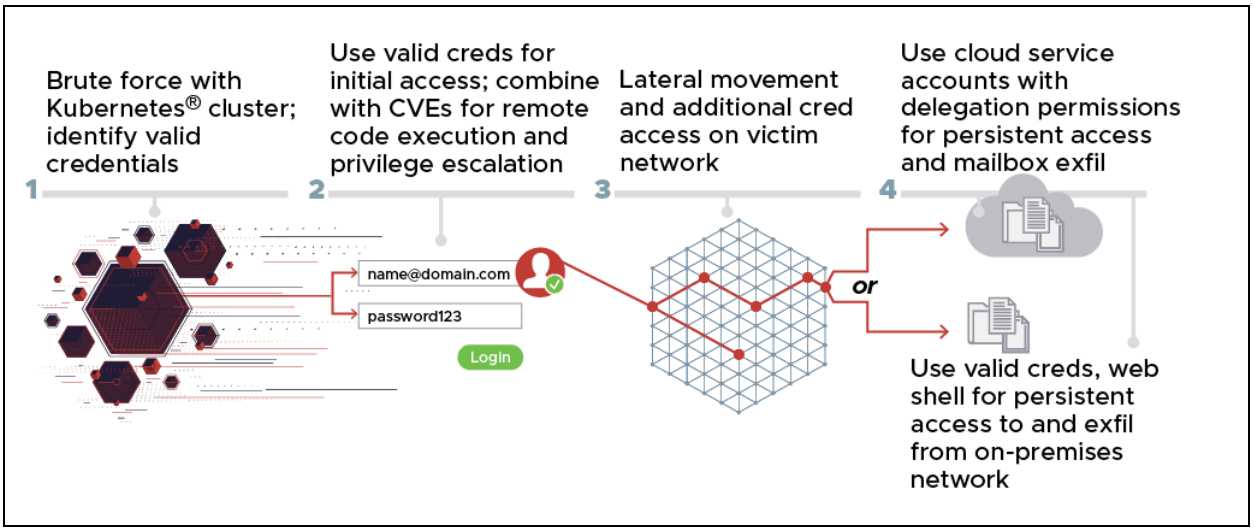

Figure 1: Example of several TTPs used together as part of this type of brute force campaign

The following table summarizes the known TTPs used in conjunction with the password spray capability. As the structure of target networks can vary greatly, the 85th GTsSS may employ a subset of these TTPs, or other TTPs not included in this summary, against different victims.

Table I: Summary of known tactics, techniques, and procedures

Tactic	Technique	Procedure/Comments
Initial Access	T1190[1] - Exploitation of Public Facing Applications	The actors used a variety of public exploits, including CVE 2020-0688 and CVE 2020-17144 to gain privileged remote code execution on vulnerable Microsoft Exchange servers. In some cases, this exploitation occurred after valid credentials were identified by password spray, as these vulnerabilities require authentication as a valid user.
Initial Access, Persistence and Privilege Escalation	T1078 - Valid Accounts	The actors used legitimate credentials, obtained through various means, to maintain access to target networks.
Persistence	T1078.002 - Valid Accounts: Cloud Accounts	The actors used a compromised Office 365 service account with Global Administrator privileges to collect email from user inboxes.
Persistence	T1505.003 – Web shell	The actors used a modified and obfuscated version of the reGeorg web shell to maintain persistent access on a target's Outlook Web Access (OWA®) server.

[1] T1190 and similar references are MITRE ATT&CK® techniques and tactics. MITRE and ATT&CK are registered trademarks of The MITRE Corporation.

Tactic	Technique	Procedure/Comments
Persistence	T1098.002 - Account Manipulation: Exchange Email Delegate Permissions	The actors used a Powershell® cmdlet (New-ManagementRoleAssignment) to grant the 'ApplicationImpersonation' role to a compromised account.
Credential Access	T1110.003 - Password Spray	The actors operate a Kubernetes cluster, which allows them to conduct distributed and large-scale targeting using password spray and password guessing.
Credential Access	T1003.001 - LSASS Memory	The actors dumped LSASS process memory by using rundll32.exe to execute the MiniDump function exported by the native Windows® DLL comsvcs.dll.
Credential Access	T1003.003 - NTDS	The actors used the ntdsutil.exe utility, which was present on a target's Active Directory® server to export the Active Directory database for credential access.
Remote Services	T1021.002 - SMB/Windows Admin Shares	The actors mapped network drives using 'net use' and administrator credentials.
Collection	T1560.001 - Archive Collected Data: Archive via Utility	The actors used a variety of utilities, including publicly available versions of WinRAR®, to archive collected data with password protection.
Collection	T1005 - Data from Local System	The actors collected files from local systems.
Collection	T1039 - Data from Network Shared Drive	The actors collected files located on a network shared drive.
Collection	T1213 - Data from Information Repositories	The actors collected files from various information repositories.
Collection	T1074.002 - Remote Data Staging	The actors staged archives of collected data on a target's OWA server.
Collection	T1114.002 - Remote Email Collection	The actors collected email from Office 365 using a compromised valid service account with elevated privileges.
Command and Control	T1115 - Ingress Tool Transfer	The actors used certutil.exe, a known "Living Off the Land" technique, to transfer a file into a target environment.
Defense Evasion	T1036 - Masquerading	The actors renamed archive files containing exfiltration data with innocuous looking names and extensions (e.g. .wav and .mp4) to resemble benign files.

Tactic	Technique	Procedure/Comments
Defense Evasion	T1036.003 - Masquerading: Rename System Utilities	The actors renamed the WinRAR utility to avoid detection.
Defense Evasion	T1036.005 - Match Legitimate Name or Location	The actors named one instance of their web shell 'outlookconfiguration.aspx' likely for the purpose of appearing to be a legitimate webpage on a targeted OWA server.
Exfiltration	T1048.002 - Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	The actors downloaded archives of collected data previously staged on a target's OWA server via HTTPS.
Exfiltration	T1030 - Data Transfer Size Limits	The actors split some archived exfiltration files into chunks smaller than 1MB.

Detection and mitigation

In an attempt to obfuscate its true origin and to provide a degree of anonymity, the Kubernetes cluster normally routes brute force authentication attempts through TOR and commercial VPN services, including CactusVPN, IPVanish®, NordVPN®, ProtonVPN®, Surfshark®, and WorldVPN. Authentication attempts that did not use TOR or a VPN service were also occasionally delivered directly to targets from nodes in the Kubernetes cluster.

The scalable nature of the password spray capability means that specific indicators of compromise (IOC) can be easily altered to bypass IOC-based mitigation. In addition to blocking activity associated with the specific indicators listed in this Cybersecurity Advisory, organizations should consider denying all inbound activity from known TOR nodes and other public VPN services to exchange servers or portals where such access is not associated with typical use.

IP addresses

Although the exact makeup of the Kubernetes cluster may change over time, a number of nodes have been identified as responsible for sending and routing the brute force authentication attempts. At some point between November 2020 and March 2021, the following IP addresses were identified as corresponding to nodes in the Kubernetes cluster:

- 158.58.173[.]40
- 185.141.63[.]47
- 185.233.185[.]21
- 188.214.30[.]76
- 195.154.250[.]89
- 93.115.28[.]161
- 95.141.36[.]180
- 77.83.247[.]81
- 192.145.125[.]42
- 193.29.187[.]60

User agents

In cases where HTTP was the underlying protocol used to deliver authentication requests, the actors used many different User-Agent strings, which are crafted to appear consistent with those sent by legitimate client software. Some of the User-Agent strings delivered in the authentication requests are incomplete or truncated versions of legitimate User-Agent strings, offering the following unique detection opportunities:

- 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.'
- 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36'
- 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0'
- 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36'
- 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_1) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.1 Safari/605.1.15'
- 'Microsoft Office/14.0 (Windows NT 6.1; Microsoft Outlook 14.0.7162; Pro'
- 'Microsoft Office/14.0 (Windows NT 6.1; Microsoft Outlook 14.0.7166; Pro)'
- 'Microsoft Office/14.0 (Windows NT 6.1; Microsoft Outlook 14.0.7143; Pro)'
- 'Microsoft Office/15.0 (Windows NT 6.1; Microsoft Outlook 15.0.4605; Pro)'

Yara rule

The following Yara rule matches the reGeorg variant web shell used by the actors. As this is a publicly available web shell, the rule does not uniquely identify 85th GTsSS malicious activity.[3]

```
rule reGeorg_Variant_Web shell {
 strings:
 $pageLanguage = "<%@ Page Language=\"C#\""
```

```
 $obfuscationFunction = "StrTr"
 $target = "target_str"
 $IPcomms = "System.Net.IPEndPoint"
 $addHeader = "Response.AddHeader"
 $socket = "Socket"
 condition:
 5 of them
}
```

General mitigations

As with mitigations for other credential theft techniques, organizations can take the following measures to ensure strong access control:

- Use multi-factor authentication with strong factors and require regular re-authentication[4]. Strong authentication factors are not guessable, so they would not be guessed during brute force attempts.
- Enable time-out and lock-out features whenever password authentication is needed. Time-out features should increase in duration with additional failed login attempts. Lock-out features should temporarily disable accounts after many consecutive failed attempts. This can force slower brute force attempts, making them infeasible.
- Some services can check passwords against common password dictionaries when users change passwords, denying many poor password choices before they are set. This makes brute-force password guessing far more difficult.
- For protocols that support human interaction, utilize captchas to hinder automated access attempts.
- Change all default credentials and disable protocols that use weak authentication (e.g., clear-text passwords, or outdated and vulnerable authentication or encryption protocols) or do not support multi-factor authentication. Always configure access controls on cloud resources carefully to ensure that only well-maintained and well-authenticated accounts have access[5].
- Employ appropriate network segmentation and restrictions to limit access and utilize additional attributes (such as device information, environment, access path) when making access decisions, with the desired state being a Zero Trust security model[6].
- Use automated tools to audit access logs for security concerns and identify anomalous access requests.

Works cited

[1] Norwegian Police Security Service (PST), “Datainnbruddet mot Stortinget er ferdig etterforsket,” December 8, 2020. https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

[2] Microsoft Threat Intelligence Center (MSTIC), “STRONTIUM: Detecting new patterns in credential harvesting.” September 10, 2020. https://www.microsoft.com/security/blog/2020/09/10/strontium-detecting-new-patters-credential-harvesting/

[3] National Security Agency, “Detect and Prevent Web Shell Malware.” April 22, 2020. https://www.nsa.gov/cybersecurity-guidance

[4] National Security Agency, “Selecting Secure Multi-factor Authentication Solutions.” October 16, 2020. https://www.nsa.gov/cybersecurity-guidance

[5] National Security Agency, “Mitigating Cloud Vulnerabilities.” January 22, 2020. https://www.nsa.gov/cybersecurity-guidance

[6] National Security Agency, “Embracing a Zero Trust Security Model.” February 25, 2021. https://www.nsa.gov/cybersecurity-guidance

Disclaimer of warranties and endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Trademark recognition

Active Directory, Microsoft Exchange, Office 365, Office, Outlook, OWA, Powershell, Windows, and Windows NT® are registered trademarks of Microsoft Corporation. • Kubernetes is a registered trademark of the Linux Foundation. • WinRAR is a registered trademark of Roshal, Alexander. • IPVanish is a registered trademark of Mudhook Marketing, Inc. • NordVPN is a registered trademark of NORDSEC PLC. • ProtonVPN is a registered trademark of Proton Technologies AG. • Surfshark is a registered trademark of SURFSHARK LTD. • Firefox® and Mozilla® and are registered trademarks of Mozilla Foundation. • Chrome® is a registered trademark of Google, Inc. • Mac® and WebKit® are registered trademarks of Apple, Inc.

Purpose

This document was developed by NSA, CISA, FBI, and NCSC in furtherance their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact information

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov