https://us-cert.cisa.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf

Reference Number: AR-17-20045

February 10, 2017

Enhanced Analysis of GRIZZLY STEPPE Activity

Executive Summary

The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) has collaborated with interagency partners and private-industry stakeholders to provide an Analytical Report (AR) with specific signatures and recommendations to detect and mitigate threats from GRIZZLY STEPPE actors.

Recommended Reading about GRIZZLY STEPPE

DHS recommends reading multiple bodies of work concerning GRIZZLY STEPPE. While DHS does not endorse any particular company or their findings, we believe the breadth of literature created by multiple sources enhances the overall understanding of the threat. DHS encourages analysts to review these resources to determine the level of threat posed to their local network environments. DHS Resources JAR-16-20296 provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. JAR-16-20296 remains a useful resource for understanding APT28 and APT29 use of the cyber kill chain and exploit targets. Additionally, JAR-16-20296 discusses some of the differences in activity between APT28 and APT29. This AR primarily focuses on APT28 and APT29 activity from 2015 through 2016.

DHS Malware Initial Findings Report (MIFR)-10105049UPDATE 2 was updated January 27, 2017 to provide additional analysis of the artifacts identified in JAR 16-20296. The artifacts analyzed in this report include 17 PHP files, 3 executables and 1 RTF file. The PHP files are webshells designed to provide a remote user an interface for various remote operations. The RTF file is a malicious document designed to install and execute a malicious executable. However, DHS recommends that analysts read the MIFR in full to develop a better understanding of how the GRIZZLY STEPPE malware executes on a system, which, in turn, downloads additional malware and attempts to extract cached passwords. The remaining two executables are Remote Access Tools (RATs) that collect host information, including digital certificates and private keys, and provide an actor with remote access to the infected system.

Open Source

Several cyber security and threat research firms have written extensively about GRIZZLY STEPPE. DHS encourages network defenders, threat analysts, and general audiences to review publicly available information to develop a better understanding of the tactics, techniques, and procedures (TTPs) of APT28 and APT29 and to potentially mitigate against GRIZZLY STEPPE activity. The below

examples do not constitute an exhaustive list. The U.S. Government does not endorse or support any particular product or vendor.

Utilizing Cyber Kill Chain for Analysis

DHS analysts leverage the Cyber Kill Chain model to analyze, discuss, and dissect malicious cyber activity. The phases of the Cyber Kill Chain are Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on the Objective. This section will provide a high-level overview of GRIZZLY STEPPE activity within this framework.

Reconnaissance

GRIZZLY STEPPE actors use various reconnaissance methods to determine the best attack vector for compromising their targets. These methods include network vulnerability scanning, credential harvesting, and using "doppelganger" (also known as "typo-squatting") domains to target victim organizations. The doppelganger domains can be used for reconnaissance when users incorrectly type in the web address in a browser or as part of delivery as a URL in the body of a phishing emails. DHS recommends that network defenders review and monitor their networks for traffic to sites that look similar to their own domains. This can be an indicator of compromise that should trigger further research to determine whether a breach has occurred. Often, these doppelganger sites are registered to suspicious IP addresses. For example, a site pretending to be an organization's User Log In resolving to a TOR node IP address may be considered suspicious and should be researched by the organization's security operations center (SOC) for signs of users navigating to that site. Because these doppelganger sites normally mimic the targeted victim's domain, they were not included in JAR-16-20296.

Before the 2016 U.S. election, DHS observed network scanning activity that is known as reconnaissance. The IPs identified performed vulnerability scans attempting to identify websites that are vulnerable to cross-site scripting (XSS) or Structured Query Language (SQL) injection attacks. When GRIZZLY STEPPE actors identify a vulnerable site, they can then attempt to exploit the identified vulnerabilities to gain access to the targeted network. Network perimeter scans are often a precursor to network attacks and DHS recommends that security analysts identify the types of scans carried out against their perimeters. This information can aid security analysts in identifying and patching vulnerabilities in their systems.

Another common method used by GRIZZLY STEPPE is to host credential-harvesting pages as seen in Step 4 and Step 5 of the GRIZZLY STEPPE attack lifecycle graphic. This technique includes hosting a temporary website in publicly available infrastructure (i.e., neutral space) that users are directed to via spear-phishing emails. Users are tricked into entering their credentials in these temporary sites, and GRIZZLY STEPPE actors gain legitimate credentials for users on the targeted network.

Weaponization

GRIZZLY STEPPE actors have excelled at embedding malicious code into a number of file types as part of their weaponization efforts. In 2014, it was reported that GRIZZLY STEPPE actors were wrapping legitimate executable files with malware (named"OnionDuke") to increase the chance of bypassing security controls. Since weaponization actions occur within the adversary space, there is little that

can be detected by security analysts during this phase. APT28 and APT29 weaponization methods have included:

- Code injects in websites as watering hole attacks
- Malicious macros in Microsoft Office files
- Malicious Rich Text Format (RTF) files with embedded malicious flash code

Delivery

As described in JAR-16-20296 and numerous publicly available resources, GRIZZLY STEPPE actors traditionally use spear-phishing emails to deliver malicious attachments or URLs that lead to malicious payloads. DHS recommends that network defenders conduct analysis of their systems to identify potentially malicious emails involving variations on GRIZZLY STEPPE themes. Inbound emails subjects should be reviewed for the following commonly employed titles, text, and themes:

- efax, e-Fax, efax #100345 (random sequence of numbers)
- PDF, PFD, Secure PDF
- Topics from current events (e.g., "European Parliament statement on...")
- Fake Microsoft Outlook Web Access (OWA) log-in emails
- Invites for cyber threat events

Additionally, GRIZZLY STEPPE actors have infected pirated software in torrent services and leveraged TOR exit nodes to deliver to malware since at least 2014. These actors are capable of compromising legitimate domains and services to host and deliver malware in an attempt to obscure their delivery methods. DHS notes that the majority of TOR traffic is not GRIZZLY STEPPE activity. The existence of a TOR IP in a network log only indicates that network administrators should review the related traffic to determine if it is legitimate activity for that specific environment.

Exploitation

GRIZZLY STEPPE actors have developed malware to exploit a number of Common Vulnerability and Exposures (CVEs). DHS assesses that these actors commonly target Microsoft Office exploits due to the high likelihood of having this software installed on the targeted hosts.

While not all-encompassing, the following CVEs have been targeted by GRIZZLY STEPPE actors in past attacks.

- CVE-2016-7855: Adobe Flash Player Use-After-Free Vulnerability
- CVE-2016-7255: Microsoft Windows Elevation of Privilege Vulnerability
- CVE-2016-4117: Adobe Flash Player Remoted Attack Vulnerability
- CVE-2015-1641: Microsoft Office Memory Corruption Vulnerability
- CVE-2015-2424: Microsoft PowerPoint Memory Corruption Vulnerability
- CVE-2014-1761: Microsoft Office Denial of Service (Memory Corruption)
- CVE-2013-2729: Integer Overflow in Adobe Reader and Acrobat vulnerability
- CVE-2012-0158: ActiveX Corruption Vulnerability for Microsoft Office
- CVE-2010-3333: RTF Stack Buffer Overflow Vulnerability for Microsoft Office
- CVE-2009-3129: Microsoft Office Compatibility Pack for Remote Attacks

Installation

GRIZZLY STEPPE actors have leveraged several different types of implants in the past. Analysts can research these implants by reviewing open-source reporting on malware families including Sofacy, and OnionDuke. Recently, DHS analyzed 17 PHP files, 3 executables, and 1 RTF file attributed to GRIZZLY STEPPE actors and the findings are located in MIFR-10105049-Update2(updated on 1/26/2017). The PHP files are webshells designed to provide a user interface for various remote operations. The RTF file is a malicious document designed to install and execute a malicious executable. DHS recommends that security analysts review their systems for unauthorized webshells.

Command andControl

GRIZZLY STEPPE actors leverage their installed malware through Command and Control (C2) infrastructure, which they traditionally develop via compromised sites and publicly available infrastructure, such as TOR. C2 IOCs are traditionally the IP addresses or domains that are leveraged to send and receive commands to and from malware implants.

Actions on the Objective

GRIZZLY STEPPE actors have leveraged their malware in multiple campaigns with various end goals. GRIZZLY STEPPE actors are capable of utilizing their malware to conduct extensive data exfiltration of sensitive files, emails, and user credentials. Security operation center (SOC)analysts may be able to detect actions on the objective before data exfiltration occurs by looking for signs of files and user credential movement within their network.

Detection and Response

The appendixes of this Analysis Report provide detailed host and network signatures to aid in detecting and mitigating GRIZZLY STEPPE activity. This information is broken out by actor and implant version whenever possible. MIFR-10105049UPDATE2provides additional YARA rules and IOCs associated with APT28 and APT29 actors.

Note: the below sections were removed due to a lack of TTPS or unclear attribution between APT28 and APT29.

APPENDIX A: APT28

APPENDIX B: APT29

APPENDIX C: Mitigations Guidance

APPENDIX D: Malware Initial Findings Report (MIFR)-10105049

ID	Name	Description
T1046	Network Service Scanning	These methods include network vulnerability scanning, credential harvesting, and using “doppelganger” (also known as “typo-squatting”) domains to target victim organizations.
TA0006	Credential Access	These methods include network vulnerability scanning, credential harvesting, and using “doppelganger” (also known as “typo-squatting”) domains to target victim organizations.
T1328	Buy domain name	These methods include network vulnerability scanning, credential harvesting, and using “doppelganger” (also known as “typo-squatting”) domains to target victim organizations.
T1566.002	Phishing: Spearphishing Link	The doppelganger domains can be used for reconnaissance when users incorrectly type in the web address in a browser or as part of delivery as a URL in the body of a phishing emails. Another common method used by GRIZZLY STEPPE is to host credential-harvesting pages as seen in Step 4 and Step 5 of the GRIZZLY STEPPE attack lifecycle graphic. This technique includes hosting a temporary website in publicly available infrastructure (i.e., neutral space) that users are directed to via spear-phishing emails. As described in JAR-16-20296 and numerous publicly available resources, GRIZZLY STEPPE actors traditionally use spear-phishing emails to deliver malicious attachments or URLs that lead to malicious payloads.
T1190	Exploit Public-Facing Application	The IPs identified performed vulnerability scans attempting to identify websites that are vulnerable to cross-site scripting (XSS) or Structured Query Language (SQL) injection attacks. APT28 and APT29 weaponization methods have included: • Code injects in websites as watering hole attacks • Malicious macros in Microsoft Office files • Malicious Rich Text Format (RTF) files with embedded malicious flash code
T1078	Valid Accounts	Another common method used by GRIZZLY STEPPE is to host credential-harvesting pages as seen in Step 4 and Step 5 of the GRIZZLY STEPPE attack lifecycle graphic. This technique includes hosting a temporary website in publicly available infrastructure (i.e., neutral space) that users are directed to via spear-phishing emails.

T1204.002	User Execution: Malicious File	In 2014, it was reported that GRIZZLY STEPPE actors were wrapping legitimate executable files with malware (named“OnionDuke”) to increase the chance of bypassing security controls. APT28 and APT29 weaponization methods have included: • Code injects in websites as watering hole attacks • Malicious macros in Microsoft Office files • Malicious Rich Text Format (RTF) files with embedded malicious flash code Additionally, GRIZZLY STEPPE actors have infected pirated software in torrent services and leveraged TOR exit nodes to deliver to malware since at least 2014. These actors are capable of compromising legitimate domains and services to host and deliver malware in an attempt to obscure their delivery methods.
T1554	Compromise Client Software Binary	In 2014, it was reported that GRIZZLY STEPPE actors were wrapping legitimate executable files with malware (named“OnionDuke”) to increase the chance of bypassing security controls. Additionally, GRIZZLY STEPPE actors have infected pirated software in torrent services and leveraged TOR exit nodes to deliver to malware since at least 2014. These actors are capable of compromising legitimate domains and services to host and deliver malware in an attempt to obscure their delivery methods.
T1137.001	Office Application Startup: Office Template Macros	APT28 and APT29 weaponization methods have included: • Code injects in websites as watering hole attacks • Malicious macros in Microsoft Office files • Malicious Rich Text Format (RTF) files with embedded malicious flash code
T1566.001	Phishing: Spearphishing Attachment	As described in JAR-16-20296 and numerous publicly available resources, GRIZZLY STEPPE actors traditionally use spear-phishing emails to deliver malicious attachments or URLs that lead to malicious payloads.
T1189	Drive-by Compromise	Additionally, GRIZZLY STEPPE actors have infected pirated software in torrent services and leveraged TOR exit nodes to deliver to malware since at least 2014. These actors are capable of compromising legitimate domains and services to host and deliver malware in an attempt to obscure their delivery methods.

T1102	Web Service	GRIZZLY STEPPE actors leverage their installed malware through Command and Control (C2) infrastructure, which they traditionally develop via compromised sites and publicly available infrastructure, such as TOR.
T1090.003	Proxy: Multi-hop Proxy	GRIZZLY STEPPE actors leverage their installed malware through Command and Control (C2) infrastructure, which they traditionally develop via compromised sites and publicly available infrastructure, such as TOR.
TA0010	Exfiltration	GRIZZLY STEPPE actors are capable of utilizing their malware to conduct extensive data exfiltration of sensitive files, emails, and user credentials.