https://www.carbonblack.com/blog/the-dukes-of-moscow/

The Dukes of Moscow

March 26, 2020

Overview

APT29, also known as The Dukes or Cozy Bear, is a cyberespionage group active since at least 2008. It's believed that the group operates either under the Russian Foreign Intelligence Service (SVR) or the Russian Federal Security Service (FSB). They primarily target western governments and related organizations. Targets include government ministries, government agencies, political think tanks, and even governmental subcontractors.

With an upcoming election in the United States, and the history of APT29 targeting western governments, it's a good time to review some of the more recent campaigns from APT29. APT29 is an extremely stealthy threat group. As much as possible they attempt to blend their network traffic in with other legitimate traffic. They do this by using compromised servers as their Command and Control (C2) infrastructure as well as using social media sites to deliver C2 messages. They have often used encrypted data in images to both deliver messages and help blend in.

In this post we take a look at some of the notable campaigns that have been discovered since 2015 up to the present day as well as the malware used in these more recent campaigns.

Timeline

2008 – 2015

F-Secure's The Dukes whitepaper provides great coverage of the history of the group between 2008 and 2015. Some of the notable early campaigns are as follows:

A campaign aimed at gathering information about Georgia-NATO relations

Exploitation of an Adobe 0-day vulnerability (CVE-2013-0640 and CVE-2013-0641) to target organizations in Ukraine, Belgium, Portugal, Romania, the Czech Republic, Ireland, the United States and Hungary

Delivering malware via a malicious Tor exit node

A high volume spear phishing campaign using e-fax themed spam usually only seen in crimeware or ransomware campaigns

2016

In June of 2016 it was discovered that APT29 had successfully breached and exfiltrated data from Democratic National Committee (DNC) servers. Crowdstrike performed an investigation and it was determined that APT29 had most likely been present in the DNC servers for at least a year. Additionally it was determined that APT28 had also breached the network. APT29 was primarily using the SeaDuke malware as part of the attack.

In August of 2016 Volexity detected a wave of spear phishing attempts against humanitarian non-governmental organizations (NGOs) and think tanks. Volexity believes this targeting initially began in 2015 but continued up to the 2016 election. Shortly after the 2016 election closed a new email phishing campaign was discovered very similar to the attempts from August of 2016. Both times the emails were attempting to distribute a PowerDuke malware variant.

2017

In February of 2017 the Norwegian Police Security Service (PST) reported on attempts to spearphish multiple individuals within the Ministry of Defence, Ministry of Foreign Affairs, and the Labour Party. These spear phishing attempts were attributed to APT29.

Also in 2017 it was revealed that attempts were made by APT29 to hack into the Dutch Ministries. Targeted phishing attempts were made by APT29 to obtain credentials for government employees in the Dutch Ministries.

2018

Most of 2018 was relatively quiet in regards to APT29 activity. In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible.

2019

In October of 2019 ESET released a report on what they called Operation Ghost. They noted that targets in the attacks varied from the Ministry of Foreign Affairs in at least three different countries in Europe as well as the Washington, DC embassy of a European Union country. In this case four new malware families were identified with enough similarities to previous APT29 tools that it was concluded these new attacks were most likely also carried out by APT29.

Malware Families

First we will take a look at each malware family used in the recent campaigns. Then we will cover common functionality used by multiple malware families that can possibly be used to detect new unknown samples.

SeaDuke

SeaDuke was used in the 2016 DNC breaches. It's written in python and compiled with PyInstaller. It communicates over HTTP using RC4 to encrypt its information and passes it across to the server in a base64 encoded cookie value. According to a report by Palo Alto Networks, The malware provides the ability to download and upload files and execute new payloads.

PowerDuke

PowerDuke was part of the spear phishing campaign in 2016 targeting NGOs and think tanks. It was delivered via email as malicious LNK files which executed PowerShell to then drop the PowerDuke backdoor. The backdoor itself was a DLL file executed from rundll32. It supports remote information gathering of the machines it's been installed on.

MiniDuke

MiniDuke has been around since at least 2010. It consists of a downloader component as well as some backdoor functionality. Some parts of MiniDuke obtain its C2 information from Twitter. Interestingly, the malware is coded in assembly. The most recent samples provide the same basic functionality as the older ones but include additional obfuscation in the form of control-flow flattening. This also has the side effect of increasing the overall size of the newer samples.

PolyglotDuke

PolyglotDuke is a downloader. ESET noted that when they encountered PolyglotDuke, it was being used to download Miniduke. PolyglotDuke acts as the initial component to install the second stage payload. It will reach out to Twitter to retrieve its real C2 address. After some initial communication with the C2 server PolyglotDuke will download an image from the C2 server over HTTP. The image retrieved is a valid image with extra RC4 encrypted data appended at the end.

RegDuke

RegDuke is a first stage implant. Its purpose is to ensure access to a machine isn't lost by staying undetected as long as possible. It is written using the .NET framework and is composed of a loader as well as a payload. The payload is a backdoor that uses Dropbox as its C2 server. The backdoor will regularly connect to a specific Dropbox account and look for PNG files to download. In this case the malicious payload is embedded within the image data itself. Data is stored in the least significant bits of each pixel and the malware can then extract the data. It then AES decrypts the data using a hardcoded key.

LiteDuke

LiteDuke is a third stage backdoor. It appears to use the same dropper as PolyglotDuke. Its payload makes use of an AES encrypted SQLite database to store its configuration. LiteDuke supports a large number of individual commands including host information retrieval, file upload and download, and the ability to execute other code. LiteDuke C2 servers appear to be compromised servers, and the malware communicates with them using normal HTTP requests. It attempts to use a realistic User-Agent string to blend in better with normal HTTP traffic.

FatDuke

FatDuke is the current third stage backdoor being used by APT29. It is dropped by MiniDuke. FatDuke has its configuration contained in the PE files resource section. It's stored as a base64 encoded JSON string. FatDuke supports C2 communication over HTTP or named pipes on the local network. Like LiteDuke, when FatDuke communicates using HTTP, it attempts to get the User-Agent string from the installed browser so that its traffic blends in better with normal HTTP traffic. FatDuke downloads malicious image files from the C2 server in order to decrypt its commands. The image files contain a corrupt PNG header and instead contains AES encrypted data from the C2 server.

Common String Encryption

The most recent samples of APT29 malware seem to make use of a common string encryption routine. This encryption routine was used as far back as 2013 in an OnionDuke sample (19972cc87c7653aff9620461ce459b996b1f9b030d7c8031df0c8265b73f670d). The strings are encoded as a sequence of hexadecimal digits. Every two hexadecimal digits decode into a single character. For example, with d35b448d9c5b6c95, there are 16 hexadecimal characters and, when decoded, we get the string “Software”.

The string decryption routine is interesting because it makes use of the srand() and rand() API calls to provide a deterministic constant used in the decryption of each character. The srand call is used to seed the pseudo-random number generator and is seeded with the malware's compilation timestamp. Then during each iteration of the string decryption loop rand will be called and that number will be used to decode the character.

The algorithm works as follows. Loop through every two characters in the encrypted string. Convert each hexadecimal ascii character to its decimal equivalent. Call rand and then perform the following computation:

character = 16 * hex1 + hex2 – rand()

This is converting the two ascii hex digits into its decimal equivalent and then subtracting the random number.

As mentioned before this string encryption is used in old OnionDuke samples but also used in PolyglotDuke, LiteDuke and FatDuke. A python routine to decrypt the strings can be seen below:

Detection

Given the level of sophistication of APT29 malware, detection can be a challenge. The malware attempts to blend in with normal network traffic as much as possible. This is done with a handful of different tactics. Communication is often done with the HTTP protocol. Some of the malware will attempt to use realistic looking User-Agent strings with the requests. The websites contacted can be various popular social media sites as well as real websites that have been compromised. Finally in the most sophisticated samples the payloads are simply image files retrieved which might look like a normal request from a web browser loading images on a page. All of these tactics contribute to the network traffic looking very similar to typical web browsing traffic.

While the network traffic itself might be hard to notice amidst all the other requests going on in your network, if you’re monitoring your endpoints it might be more noticeable. For instance, in some cases the droppers are writing the malicious backdoors to disk as a DLL and then executing them using rundll32. On the endpoint monitoring side, seeing a process like rundll32 making connections to popular web sites like Twitter or Dropbox is probably not going to be something that typically happens. This in combination with detecting untrusted new files being executed can be some of the best ways to detect this malware.

Conclusion

Since 2015 APT29 has continued its targeted campaigns against governments and related organizations. Their stealthy network communication tactics and obfuscated binaries make them hard to detect. With another U.S. election coming up it’s safe to say that we will continue to see

APT29 attempting to target government entities here in the U.S. as well as around the globe. We will continue to monitor their activity to provide insight and information to our customers.

ID	Name	Description
TA0011	Command and Control	They do this by using compromised servers as their Command and Control (C2) infrastructure as well as using social media sites to deliver C2 messages. LiteDuke C2 servers appear to be compromised servers, and the malware communicates with them using normal HTTP requests.
T1102	Web Service	They do this by using compromised servers as their Command and Control (C2) infrastructure as well as using social media sites to deliver C2 messages. MiniDuke has been around since at least 2010. It consists of a downloader component as well as some backdoor functionality. Some parts of MiniDuke obtain its C2 information from Twitter. PolyglotDuke acts as the initial component to install the second stage payload. It will reach out to Twitter to retrieve its real C2 address. RegDuke - The payload is a backdoor that uses Dropbox as its C2 server. The backdoor will regularly connect to a specific Dropbox account and look for PNG files to download. In this case the malicious payload is embedded within the image data itself. Data is stored in the least significant bits of each pixel and the malware can then extract the data. It then AES decrypts the data using a hardcoded key.
T1001.002	Data Obfuscation: Steganography	They have often used encrypted data in images to both deliver messages and help blend in. After some initial communication with the C2 server PolyglotDuke will download an image from the C2 server over HTTP. The image retrieved is a valid image with extra RC4 encrypted data appended at the end. RegDuke - The payload is a backdoor that uses Dropbox as its C2 server. The backdoor will regularly connect to a specific Dropbox account and look for PNG files to download. In this case the malicious payload is embedded within the image data itself. Data is stored in the least significant bits of each pixel and the malware can then extract the data. It then AES decrypts the data using a hardcoded key.

		FatDuke downloads malicious image files from the C2 server in order to decrypt its commands. The image files contain a corrupt PNG header and instead contains AES encrypted data from the C2 server. Communication is often done with the HTTP protocol. Some of the malware will attempt to use realistic looking User-Agent strings with the requests. The websites contacted can be various popular social media sites as well as real websites that have been compromised. Finally in the most sophisticated samples the payloads are simply image files retrieved which might look like a normal request from a web browser loading images on a page.
T1189	Drive-by Compromise	Delivering malware via a malicious Tor exit node
T1566	Phishing	A high volume spear phishing campaign using e-fax themed spam usually only seen in crimeware or ransomware campaigns. In August of 2016 Volexity detected a wave of spear phishing attempts against humanitarian non-governmental organizations (NGOs) and think tanks. Shortly after the 2016 election closed a new email phishing campaign was discovered very similar to the attempts from August of 2016. In February of 2017 the Norwegian Police Security Service (PST) reported on attempts to spearphish multiple individuals within the Ministry of Defence, Ministry of Foreign Affairs, and the Labour Party. Targeted phishing attempts were made by APT29 to obtain credentials for government employees in the Dutch Ministries. In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. PowerDuke was part of the spear phishing campaign in 2016 targeting NGOs and think tanks. Shortly after the 2016 election closed a new email phishing campaign was discovered very similar to the attempts from August of 2016. Both times the emails were attempting to distribute a PowerDuke malware variant. In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload.

T1566.001	Phishing: Spearphishing Attachment	PowerDuke was part of the spear phishing campaign in 2016 targeting NGOs and think tanks. It was delivered via email as malicious LNK files which executed PowerShell to then drop the PowerDuke backdoor.
T1204	User Execution: Malicious File	It was delivered via email as malicious LNK files which executed PowerShell to then drop the PowerDuke backdoor.
T1059.001	Command and Scripting Interpreter: PowerShell	It was delivered via email as malicious LNK files which executed PowerShell to then drop the PowerDuke backdoor.
TA0010	Exfiltration	In June of 2016 it was discovered that APT29 had successfully breached and exfiltrated data from Democratic National Committee (DNC) servers. LiteDuke supports a large number of individual commands including host information retrieval, file upload and download, and the ability to execute other code. SeaDuke was used in the 2016 DNC breaches. It's written in python and compiled with PyInstaller. It communicates over HTTP using RC4 to encrypt its information and passes it across to the server in a base64 encoded cookie value. According to a report by Palo Alto Networks, The malware provides the ability to download and upload files and execute new payloads.
T1548.002	Abuse Elevation Control Mechanism: Bypass User Access Control	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1134.001	Access Token Manipulation: Token Impersonation/Theft	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1134.003	Access Token Manipulation: Make and Impersonate Token	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/

T1134.004	Access Token Manipulation: Parent PID Spoofing	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1071	Application Layer Protocol	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1071.001	Web Protocols	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1071.004	DNS	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1197	BITS Jobs	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1059.001	Command and Scripting Interpreter: PowerShell	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1059.003	Command and Scripting Interpreter:	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing

	Windows Command Shell	attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1059.005	Command and Scripting Interpreter: Visual Basic	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1059.006	Command and Scripting Interpreter: Python	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1543.003	Create or Modify System Process: Windows Service	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1005	Data from Local System	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1068	Exploitation for Privilege Escalation	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1070.006	Indicator Removal on Host: Timestomp	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used

		makes it seem plausible. https://attack.mitre.org/software/S0154/
T1056.001	Input Capture: Keylogging	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1185	Man in the Browser	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1106	Native API	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1046	Network Service Scanning	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1135	Network Share Discovery	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1027.005	Obfuscated Files or Information: Indicator Removal from Tools	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/

T1003.002	OS Credential Dumping: Security Account Manager	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1057	Process Discovery	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1055	Process Injection	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1055.012	Process Hollowing	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1572	Protocol Tunneling	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1090.001	Proxy: Internal Proxy	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1021.001	Remote Services: Remote Desktop Protocol	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing

		attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1021.002	Remote Services: SMB/Windows Admin Shares	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1021.003	Remote Services: Distributed Component Object Model	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1021.004	Remote Services: SSH	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1021.006	Remote Services: Windows Remote Management	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1018	Remote System Discovery	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1029	Scheduled Transfer	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used

		makes it seem plausible. https://attack.mitre.org/software/S0154/
T1113	Screen Capture	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1569.002	System Services: Service Execution	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1550.002	Use Alternate Authentication Material: Pass the Hash	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1078 .003	Valid Accounts: Local Accounts	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1078 .002	Valid Accounts: Domain Accounts	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/
T1047	Windows Management Instrumentation	In November however, FireEye reported on a possible APT29 phishing campaign targeting multiple U.S. companies and organizations. In this case the phishing attempts contained a Cobalt Strike beacon payload. While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. https://attack.mitre.org/software/S0154/

T1204.002	User Execution: Malicious File	While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible. PowerDuke was part of the spear phishing campaign in 2016 targeting NGOs and think tanks. It was delivered via email as malicious LNK files which executed PowerShell to then drop the PowerDuke backdoor.
T1059.001	Command and Scripting Interpreter: PowerShell	While the attack was not definitively attributed to APT29, the similarities in the malicious LNK files and PowerShell used makes it seem plausible.
T1059.006	Command and Scripting Interpreter: Python	SeaDuke was used in the 2016 DNC breaches. It's written in python and compiled with PyInstaller.
T1071.001	Application Layer Protocol: Web Protocols	SeaDuke was used in the 2016 DNC breaches. It's written in python and compiled with PyInstaller. It communicates over HTTP using RC4 to encrypt its information and passes it across to the server in a base64 encoded cookie value. Communication is often done with the HTTP protocol. Some of the malware will attempt to use realistic looking User-Agent strings with the requests. The websites contacted can be various popular social media sites as well as real websites that have been compromised. Finally in the most sophisticated samples the payloads are simply image files retrieved which might look like a normal request from a web browser loading images on a page. PolyglotDuke acts as the initial component to install the second stage payload. It will reach out to Twitter to retrieve its real C2 address. After some initial communication with the C2 server PolyglotDuke will download an image from the C2 server over HTTP. The image retrieved is a valid image with extra RC4 encrypted data appended at the end. LiteDuke C2 servers appear to be compromised servers, and the malware communicates with them using normal HTTP requests. LiteDuke C2 servers appear to be compromised servers, and the malware communicates with them using normal HTTP requests. It attempts to use a realistic User-Agent string to blend in better with normal HTTP traffic. FatDuke supports C2 communication over HTTP or named pipes on the local network. Like LiteDuke, when FatDuke communicates using HTTP, it attempts to get the User-Agent string from the installed browser so that its traffic blends in better with normal HTTP traffic.

T1573.001	Encrypted Channel: Symmetric Cryptography	SeaDuke was used in the 2016 DNC breaches. It's written in python and compiled with PyInstaller. It communicates over HTTP using RC4 to encrypt its information and passes it across to the server in a base64 encoded cookie value. RegDuke - The payload is a backdoor that uses Dropbox as its C2 server. The backdoor will regularly connect to a specific Dropbox account and look for PNG files to download. In this case the malicious payload is embedded within the image data itself. Data is stored in the least significant bits of each pixel and the malware can then extract the data. It then AES decrypts the data using a hardcoded key. LiteDuke is a third stage backdoor. It appears to use the same dropper as PolyglotDuke. Its payload makes use of an AES encrypted SQLite database to store its configuration. FatDuke downloads malicious image files from the C2 server in order to decrypt its commands. The image files contain a corrupt PNG header and instead contains AES encrypted data from the C2 server.
T1105	Ingress Tool Transfer	SeaDuke was used in the 2016 DNC breaches. It's written in python and compiled with PyInstaller. It communicates over HTTP using RC4 to encrypt its information and passes it across to the server in a base64 encoded cookie value. According to a report by Palo Alto Networks, The malware provides the ability to download and upload files and execute new payloads. PowerDuke was part of the spear phishing campaign in 2016 targeting NGOs and think tanks. It was delivered via email as malicious LNK files which executed PowerShell to then drop the PowerDuke backdoor. The backdoor itself was a DLL file executed from rundll32. It supports remote information gathering of the machines it's been installed on. For instance, in some cases the droppers are writing the malicious backdoors to disk as a DLL and then executing them using rundll32. LiteDuke supports a large number of individual commands including host information retrieval, file upload and download, and the ability to execute other code.
T1218.011	Signed Binary Proxy Execution: Rundll32	For instance, in some cases the droppers are writing the malicious backdoors to disk as a DLL and then executing them using rundll32.

TA0003	Persistence	MiniDuke has been around since at least 2010. It consists of a downloader component as well as some backdoor functionality.
T1027	Obfuscated Files or Information	MiniDuke has been around since at least 2010. It consists of a downloader component as well as some backdoor functionality. Some parts of MiniDuke obtain its C2 information from Twitter. Interestingly, the malware is coded in assembly. The most recent samples provide the same basic functionality as the older ones but include additional obfuscation in the form of control-flow flattening. The most recent samples of APT29 malware seem to make use of a common string encryption routine.
T1505.001	Server Software Component: SQL Stored Procedures	LiteDuke is a third stage backdoor. It appears to use the same dropper as PolyglotDuke. Its payload makes use of an AES encrypted SQLite database to store its configuration.
T1005	Data from Local System	LiteDuke supports a large number of individual commands including host information retrieval, file upload and download, and the ability to execute other code.
TA0002	Execution	LiteDuke supports a large number of individual commands including host information retrieval, file upload and download, and the ability to execute other code.