The Cybersecurity Threat Landscape Group Assignment

CMIT 495: Current Trends and Projects in Computer Networks and Security

[Michael Bartlett]

By:

[Dexter Bowling, Alvin Sarkadi]
[Joseph Azucena, Kelvin Contreras]
[Malahi Harris, Hercle Ivy]

Introduction

Part 1: Threat Landscape Analysis

In today's digital word, Information Operations has become the 5th domain considered critical during war time. This domain has continued to advance beyond the initial limitations predating the internet. Since the 1970s cyber security has transformed into a race towards education, exploitation, defense in depth and asset protection (*History of cybersecurity:* How it started, and how it's changed | Lucidum ®). Today, the Advanced Persistent Threats (APTs) have emerged as a formidable adversary in the digital landscape, characterized by their sophisticated Tactics, Techniques, and Procedures (TTPs), long-term goals, anonymity, and significant resources. An advanced persistent threat is a sophisticated and stealthy cyberattack where a malicious actor gains unauthorized access to a network and remains undetected for an extended period. (Yasar, 2023) By diligently studying how victims operate daily an attacker is able to implement creative ways of compromising a network without being detected. From there, the attacker is able to laterally maneuver through a network to perform actions on the objective. These typically consist of intellectual property and sensitive data theft, disrupt operations, and conducting espionage without being discovered. This overview with be focus on, Chinese threat actor, APT1 which has been a persistent and sophisticated threat to organizations worldwide. This analysis will delve into the threat landscape, examine the specific methods used by APT1, and explore potential countermeasures, including the applying cation of machine learning and data analytics.

APT1 excels at maintaining persistent access to compromised networks. Once inside, they employ stealthy tactics and sophisticated malware to ensure ongoing control and hidden access to victims infrastructure. This persistence allows them to operate undetected for extended periods. Its

advanced TTPs make it a formidable adversary with the capability of compromising even the most robust security stacks. Mandiant, a Security Company that investigates Cyber Security Breaches around the world, published a report in 2013 that blames the Chinese government for funding APT1. (Swain, 2023)

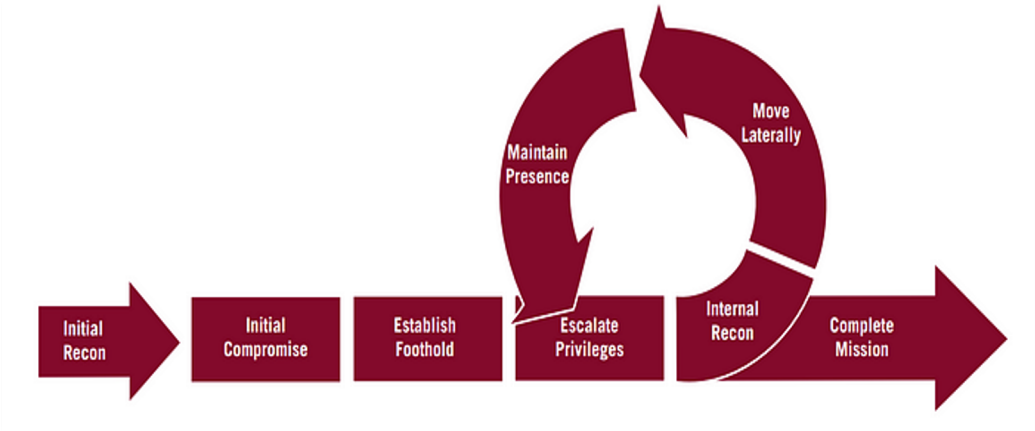

Figure 1: APT1 Mission Cycle (Khan, 2024)

Common tactics used by APT1 are Spear Phishing campaigns, malware development and deployment through backdoors, and publicly available privilege escalation tools that further help data exfiltration. Their spear-phishing emails primarily contain disguised malware attachments that have common job-related fake file extensions such as zip, jpeg, pdf, and doc. These are used to deceive victims into thinking the files are harmless and opening them on a host. The standard APT1 backdoor typically communicates using the Hyper Text Transfer Protocol (HTTP) (to blend in with legitimate web traffic) or a custom protocol that the malware authors designed themselves. In addition to this, common open source privilege escalation tools used by APT1 are cachedump, fgdump and gsecdumb. (Khan, 2024) These are only a small subset of tools used by this threat actor. They are well versed with other methods that have been a hindrance to over 100 organizations.

In 2014, five APT1 members were charged by US federal prosecutors in relation to multiple data breaches at different U.S. companies. These five chargers further prove Mandiant's reports about APT1 being state sponsored.

Figure 2: APT1 Arrest (Matt, 2020)

Recently, APT1 has resurfaced over the past two decades. Knowledge now reported that APT1 was by far the most referenced threat actor in the last seven days of September 2020. Over the past few years APT1 has even become more sophisticated and has been observed using more advanced tools and techniques, such as artificial intelligence and machine learning. AI has enabled APT1 to automate reconnaissance efforts and dynamically adapt its malware to evade detection in real time. (Infinity, 2024) On top of that the group is believed to operate with state-of-the-art technology, and numbers have grown by the thousands. APT1 target's locations like the United Sates, Europe and the Middle East. Whether its military information, strategic plans for tech companies and other sensitive data. Its targets have even expanded from just traditional government agencies but also now include strategic plans in the energy sector, aircraft designs in aerospace and infrastructure networks for transportation. (Waterhouse, 2024)

As of today, APT1 is likely to persist in exploiting vulnerabilities within common software and information systems. Its targets often include operating systems such Windows, macOS, and Linux; applications such as Microsoft Office, Adobe Acrobat, and web browsers; network devices like routers, switches, and firewalls; and cloud services including storage, email, and collaboration platforms.

Moreover, the group is expected to focus on emerging technologies, such as Internet of Things (IoT) devices, 5G networks, and as mentioned earlier, artificial intelligence (AI) and machine learning systems. (APT1, 2021) By understanding the tactics, techniques, and procedures employed by APT1, organizations can better anticipate and defend against similar threats.

Part 2: APT Analysis

APT1 describes one of Chinas espionage groups that Mandiant – an investigative security firm – that has been investigating Chinese APT groups since 2006. The firm found that the group has attacked nearly 150 victims from 2006 -2011. The investigation has led to the uncovering of four large networks in Shanghai and the groups attack infrastructure, command and control and tools/tactics and procedures with three identified "personas" in the group (*APT1: Exposing one of China's cyber espionage units*). APT1 is likely to be government sponsored and thus can wage long running and complex cyber espionage programs. Mandiant found that APT1 is also located near the Peoples Liberation Army (PLA) unit 61398 which is considered to engage in harmful computer network operations. APT1 is believed to operate under the PLA Unit 61398 running similar operations. APT1 targets also match the industries that that China had identified as strategic emerging industries in their 5-year plan (*APT1: Exposing one of China's cyber espionage units*). The firm found that APT1 has considerable infrastructure that Is not only located in China but in 13 different countries. Mandiant has observed about 937 Command and Control Servers registered to 849 IP addresses but acknowledges that this may only be a small part of the actual work that APT1 is doing.

The threat group focuses have been primarily directed towards organizations that conduct their business in English with 115 victims in the United States alone. Once APT1 has compromised a network they repeatedly steal proprietary data and monitor the victims for months or years (*APT1: Exposing one of China's cyber espionage units*). Spearfishing is their number one tactic, technique, and practice

employed to compromise organizations (*APT1: Exposing one of China's cyber espionage units*). APT1 does extensive research to penetrate a target by using real people's names and other information relevant to the recipient than plan to compromise.

Once APT1 has initiated an encounter with spearfishing, they most commonly infiltrate a network by installing a backdoor through a malicious file. A backdoor allows them to send commands remotely to an infiltrated network by communicating with a Command Control server that initiates outbound communications by malware embedded in the system (*APT1: Exposing one of China's cyber espionage units*). Once APT1 had access to a network through sophisticated backdoors, they could easily create/modify programs, upload/download files, capture keystrokes, start a command shell, harvest credentials, shutdown the system, or modify the system (*APT1: Exposing one of China's cyber espionage units*). APT1 then uses predominantly publicly available tools to dump password hashes to harvest credentials such as cachedump, mimikatz, or pass-the-hash toolkit. APT1 has been observed using scripts to dump system information into a text file such as network configuration information, running services, listed accounts, and other systems on the network (Mandiant, 2013). Once outfitted with stolen but legitimate credentials, APT1 can maintain their presence on the system by installing new backdoors on multiple systems and accessing shared network services. They frequently use scripts to then facilitate the capture of files and then move them out of the system by backdooring them or using existing file transfer protocol. APT1 is unique in the sense that they have developed proprietary email stealing utilities called GETMAIL and MAPIGET which both steal emails from Microsoft Outlook archive files. MAPIGET was designed specifically to steal email that still resides on a Microsoft Exchange Server and has not been archived yet (*APT1: Exposing one of China's cyber espionage units*). APT1 has been largely successful in the exploitation of its victims. It has stolen hundreds of terabytes of data from a minimum of 141 global organizations. It can access its victims' system for an average of 356 days and was able to stay in a network for 4 years and 10 months in its longest breach. It is sufficient to say that APT1 has been more than

successful in breaching its victims since 2006 up until this report was released in 2013. APT1s objective as an advanced persistent threat is most likely to steal sensitive information including espionage, data theft, and network disruption (*Nation-state cyber actors*). Considering APT1s targets primarily being active in emerging industries that interest China, its focus might be to steal data that can help develop Chinas own work in those emerging industries.

Part 3: Cybersecurity Tools, Tactics, and Procedures

In todays digital infrastructure there are a range of cyber security tools, tactics and procedures employed to help defend networks. Common hardware solutions involve next gen firewalls and IDS's which are often times used to help filter traffic not intended for the network. The complement to these are software solutions such as Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Security Information & Event Management Systems (SIEM) which are used to help mitigate threats that have dodged the first stage hardware defenses. Both of these solutions work collectively leveraging Cyber Threat Intelligence collection along with real time detection and response. When each of these different tactics are grouped with hardware or software solutions, procedures are set forth on how to successfully deploy them for greatest visibility. This idea today is often referenced as defense in depth since it uses a layered of approach to provide a modular cybersecurity protection. In addition to this, Identity and Access Management (IAM) is integrated along with encryption to help further protect accounts and information within an enterprise. Even with these security practices deployed, it is important to understand that they alone do not stop malicious cyber actors. Often times the will work for detecting less mature threat actors but fail at detecting advanced threat actors. We believe this is because attackers only have to be correct one time whereas defenders have to be correct 100% of the time. In addition to this is the variable of time where APTs are able to work within unconfined timeframes. This becomes relevant when systems are taken down for updates and or patches in addition to other administrative reasons. Another point worth note is understanding threat

actors are also performing their own research and due diligence to better understand what occurs under the hood within many of these security products. These are only some of the few reasons why these types of devices are not successful against APTs.

Part 4: Machine Learning and Data Analytics

Machine Learning (ML) is a branch of artificial intelligence (AI) that is used to make predictions. It allows a system to learn and make decisions without being told to. It uses a set algorithm that takes datasets, identify patterns, and makes decisions or predictions based off the data. There are three main algorithms used in Machine Learning: supervised, unsupervised, and reinforcement learning. In supervised learning the system is trained on labeled data. Each input of data has a correct output that is labeled. This allows the system to match corresponding inputs to the appropriate output. An example of this is spam email detection. Each email in the dataset has a label of either “spam” or “not spam”. The system will use this data set learn where to place incoming emails based on what it has learned. In unsupervised learning, the system is given the initial data, but it has no labels. This means that the machine must find patterns or classification in the data. A retailer could use unsupervised learning to group customers based of purchase history. The machine can place customers into a group labeling it frequent customer. This would allow the store owner to keep what the frequent customer purchases in stock. Reinforcement learning gives the system a goal to reach. While pursuing this goal, we give it feedback based on the decisions it has made. This allows the machine to improve its abilities over time. Machine learning offers powerful predictive capabilities, it is also related to data analytics, which gives it the foundational insights and patterns that fuel the algorithms.

Data analytics is the process of examining datasets and using the organized data to make informed decisions. It is often used by organizations to make financially sound decisions. There are four types of data analytics the are used to help make these decisions. Descriptive analytics tells us what happened. Diagnostic analytics lets us know why it happened. Predictive analytics tells us what can

possibly happen in the future. Prescriptive analytics tells us what actions should be taken. The reason data analytics is related to machine learning is because they only have a few differences. The main difference is the human aspect. Machine learning can make predictions or decision with explicit programming. While in data analytics, it is mainly used to help someone make the decision. We can also use these methods to evolve the cybersecurity field!

Cybersecurity involves the protection of systems, data, and networks. If machine learning and data analytics is integrated, cybersecurity can be improved in multiple ways. Traditional cybersecurity methods rely on predefined rules and signatures to identify threats. These rules and signatures can be bypassed by complex attacks. Machine Learning can analyze sizable amounts of network traffic and identify unusual patterns that may indicate emerging threats, like zero-day vulnerabilities. ML can be used to develop automated responses to detected security incidents. Real-time data analysis can be used to predict the impact of an attack and can start the proper response. The response can range from isolating the affected system or blocking questionable IP addresses. Data analytics can be used to predict vulnerabilities in systems. By understanding historical attack data and system logs, we can predict when future attacks might occur. These integrating can also help defend against long-term cyberattacks such as APT1.

APT1 tactics can be categorized as complex attacks. The attackers would infiltrate networks and remain undetected for a long period of time. They used emails with malicious attachments or links to gain an initial footing in targeted networks. They deployed custom malware to maintain control over compromised systems and exfiltrate data. Once they gained access, they moved laterally across networks to escalate privileges and access restricted data. Because they relied on lateral movement to expand their control across networks, traditional security measures might miss this. This is because the attackers often mimic legitimate user behavior. If ML was used to analyze behavior patterns, these activities could have been flagged. For instance, ML models can track typical login patterns and detect

unusual access requests. Like a low-privileged user suddenly trying to access critical systems or data. APT1 was also known for exploiting vulnerabilities in software that had not yet been patched. These are also known as zero-day vulnerabilities. Machine learning can help identify unknown vulnerabilities by detecting abnormal interactions with software. This might indicate that attackers are leveraging a zero-day exploit. Data analytics can also associate data from various sources to identify the possible existence of zero-day exploits sooner. Companies have already started to provide cybersecurity options based on these technologies.

There are multiple companies offering innovative defensive cybersecurity measures that leverage the technologies discussed previously. These companies address cyber threats such as ransomware, phishing, and advanced persistent threats (APTs). They do this by using technologies such as artificial intelligence (AI), machine learning (ML), zero-trust frameworks, blockchain, and automation. There are three companies that can be recommended. Those companies being CrowdStrike, Darktrace, and SentinelOne. CrowdStrike shines in endpoint detection, making it ideal for companies seeking scalable EDR solutions. Darktrace stands out for its autonomous, AI-driven response, making it a leader in automated network-based threat detection. SentinelOne also shines in endpoint protection like CrowdStrike. However, SentinelOne emphasizes real-time autonomous remediation. Of the three, CrowdStrike is recommended because the industry-leading Falcon platform. It leverages AI and machine learning to provide real-time endpoint detection and response (EDR). The cloud architecture is scalable, and it has excellent threat hunting capabilities. This can ensure the company stays ahead of both known and unknown cyber threats.

Part 5: Using Machine Learning and Data Analytics to Prevent APT

Before 2010, using machine learning algorithms to detect anomalies within networks was in its infancy. Instead, most available intrusion detection systems were rule based, requiring manual input. This meant rules had to be set by an administrator, and in emergency instances, manual scripts of code

would have to be deployed to detect known APTs. In Mandiant's resource paper APT 1, the attackers commonly used spear phishing, a remote access trojan known as Gh0st rat, WebC2 backdoors and many other publicly available malwares to remain persistent within any network infrastructure they attack. In the early 2000's if organizations had information about APT1, such as the malware family they were using, known hi-jacked domains, the approximate location or city and IP addresses used in the attacks, significant data analytics can be applied to intercept these attacks.

If this information was readily available to organizations in the early 2000s, tools such as Snort, Wireshark, Cisco IronPort, and Splunk could have detected anomalies in organizations networks. Data analytics may have been applied to help mitigate APT persistence and lateral movement. In Snort and many other early Intrusion Detection Systems (IDS) rules in security policies and scripts to detect APT behavior could have been made. In Mandiant's report, APT 1's spear phishing campaign involved sending attachments (.pdf .doc and zip files) or links and hyperlinks which were obfuscated to bypass any anti-virus the organization had in place. Mandiant provides examples of file names and industries they target, such as 'Updated_Office_Contact_v1.zip' 'Oil-Field-Services-Analysis-And-Outlook.zip' 'Welfare_Reform_and_Benefits_Development_Plan.zip' and much more. From this information administrators can inform employees to carefully check file names, and when sending sensitive information, deviate from the examples / file names provided. For example, if someone sends a email with an attachment to a different department, the employee should have physical contact with the employee, making sure that credentials are not stolen and malware is not present in the email. (Phone call, or in person)

Recommendations before 2010 aim to use IronPort, Snort, Wireshark, Sandbox tools and much more. IronPort is a more secure email application that can analyze any emails for malware. IronPort's email security appliance can categorize, filter, and can alert administrators about unusual file transfers.

Additionally, in Snort, alerts can be created when suspicious URL's and attachments are sent to an end device on the network. Since there is little documentation about Snort commands available in 2008, we provide a hypothetical example of how Snort would detect a suspicious attachment in an email:

```
alert any TCP-received-email-attachment.zip-attachment.pdf-
attachment.doc-output: "A zip, pdf or doc file was found in the email,
investigate"

alert any TCP-received-email-unknown-url-hyperlink-output: "A unknown
URL or hyperlink was found in the email. Investigate.
```

Figure 3: Snort Detection of Email Attachment (Snort 3 rule writing guide)

From this alert, an administrator can check whether there is any correlation to the APT threat actor's choice of naming files. If any correlation is found, then the attachment should be isolated and placed in a sandbox environment to check its behavior and see how it is able to escalate privileges. It is important to note that most of the malware used by APT1 bypasses malware signature detection, allowing it to remain persistent in sophisticated network security environments. However, using several different sandbox tools available at the time, some evidence could have been collected about malware behavior, its ability to escalate privileges, how it changes file systems.

Additionally, Snort and IronPort can work together in conjunction. In Figure 1, IronPort provides any necessary email security. If both are used in a network organization, it would be easier to identify APT 1's threats and mitigate them in the future.

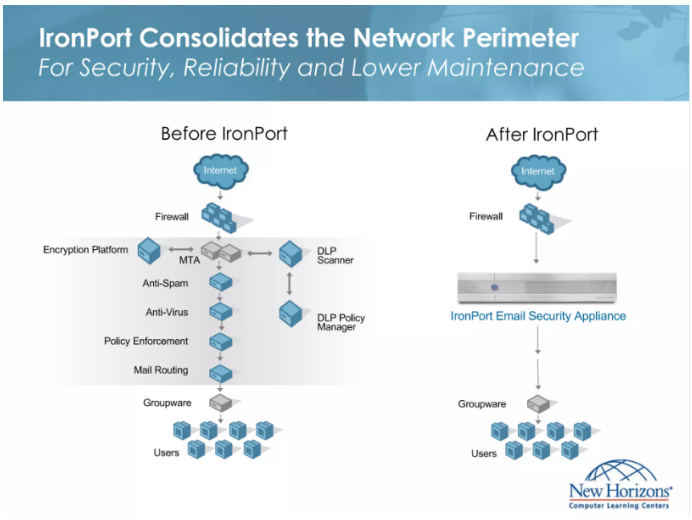

Figure 4: Email Security Implementation with IronPort (Ironport Data Loss Prevention 2009)

If Administrators of the organization still believe that their network infrastructure is at high risk of becoming a victim of APT 1, additional security training should be used for employees in organizations, reminding them to open files only when safe, in a sandbox environment, or when checked with dozens of malware signatures. Although APT 1's malware bypassed most signatures, tools like Virus total can analyze files or URLS with several security vendors, the use of Virus total could have had a significant impact. Employees should rely on encryption methods when sending sensitive organization information. Since M/L algorithms were almost not exist at the time (in the cybersecurity field), it's important for users of the organization to encrypt sensitive information in their own way. Although PGP can be seen as difficult for users to deploy, IronPort had adopted Open PGP and other encryption models so that users can access these encryption tools with ease. Using IronPort in conjunction with Snort will help the overall security posture of the network.

Sandboxing is also a significant tool when analyzing APT 1's choice of malware. Sandboxing their malware can identify its behavior and organizations can prevent it from doing harm and escalating privileges. Specifically, Cuckoo Sandbox. When you search up for sandbox applications on google several will show up, most of them will include several features such as user interaction and malware response / behavior, snapshot creation to check the system files before and after executing the malware, and much more.

Intrusion detection systems like Snort and IronPort with the correct rules and scripts, and Sandbox applications can be used to further investigate malware files. Additionally, Wireshark provides a comprehensive U.I that can detect unusual network patterns, file transfers, and more.

As previously stated, APT 1 uses malware that is difficult to identify even when using network security tools that are available. The focus should include the domains used, FTP formats for data exfiltration, finding instances of the gh0st rat on any existing system, traffic analysis through Wireshark and tracing APT 1's patterns.

One significant pattern is the use of the Chinese (Simplified) – U.S Keyboards when users of APT 1 use RDP sessions. APT 1 targets mostly English speaking based organizations. Most organizations will find that their employees will use the default keyboard option because of their English proficiency (English – United Kingdom, English – United States of America.) Administrators should block the use of the keyboard layout used by APT1 threat actors. Additionally, if Mandiant was able to identify the various domains and third party privilege escalation tools used before 2010, manual configuration and data analytics can be applied to block:

cachedump, fgdump, gsecdump,lslsass,mimikatz,pass-the-hash-toolkit,pwdump7 and pwdumpx.

Administrators can trace if any of the utilities was used to compromise any device or network. Furthermore, Mandiant provides a wide array of domains used by APT1 to disguise themselves. If the domain names were known to security employees and researchers before 2010, a network admin can block all users of the organization from accessing such domains. Due to the sophistication of APT 1's attack, traffic analysis in Wireshark should also be held to a high degree.

In this second figure, Wireshark is used to decrypt communications that involve gh0st rat. Once the TCP stream that includes gh0st rat is found and traced, it can be dumped into hexadecimal format, you should see Gh0st in the first string (If doing malware analysis, or if the organization believes they are a victim to APT 1.) This means the end device and network is infected. This should be immediately brought to the attention of the CTO, so that backup strategies can be made, and all devices should be disconnected from the network and powered off to prevent lateral movement.

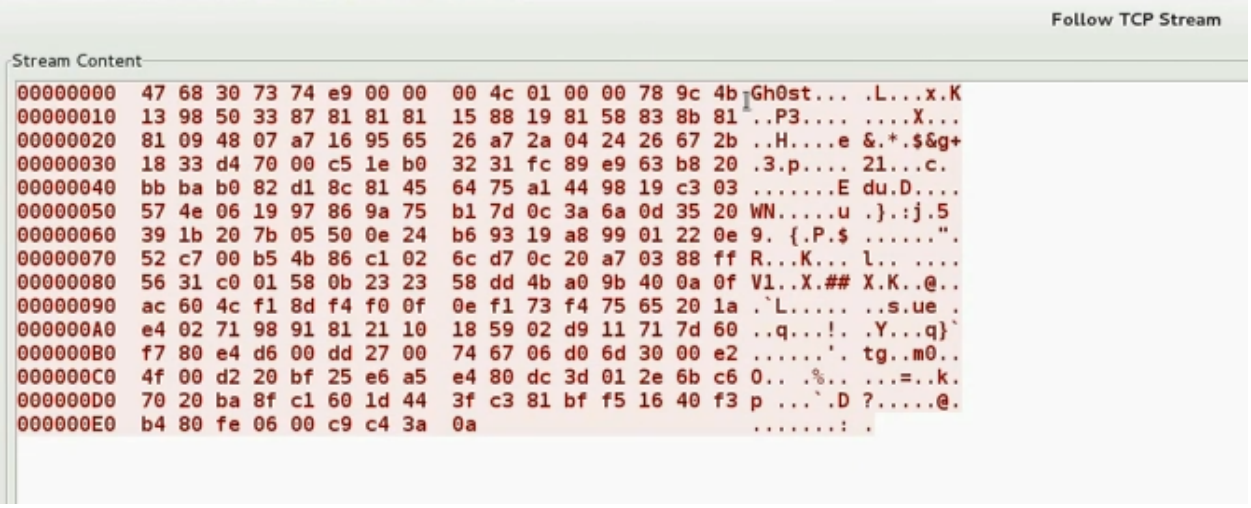

Figure 5:Wireshark – Following a TCP Stream, converting the streamed content into hex to identify the Gh0st rat

Another significant persistent pattern for APT 1 is compressing stolen data into multiple .rar files. This signifies that large amounts of data are being sent, by sending parts for one archive it's evident that APT 1 could be stealing dozens or even hundreds of terabytes of data. From Mandiant's report, we usually see that when they steal information from an organization, it's one archive but it's separated into multiple rar files. Going back to Snort, a significant utility prior to 2010 and onwards when M/L in cybersecurity was emerging. Snort could have created a script or rule to deny access to any FTP data exfiltration for .rar archives. For example, a alert code can be written, since there is little documentation on previous versions of Snort, the code would look something like this: alert tcp-MY_NETWORK port 21,20 large_data extension_rar. output: "Large amounts of data in rar archives are being moved via FTP, check immediately." The code would not look like this due to lack of resources of the first versions of

Snort, however it would be similar, alerting a user that large amounts of data are being moved on ports designated for FTP and the large data in question are .rar archives.

2010 and Beyond: K Means Clustering

After 2010, M/L algorithms started to emerge, one of them being k means clustering. This method of M/L divides unlabeled data into various groups called clusters. K means clustering can be used for several industries. A basic example is grades on a quiz. K can represent the number of clusters. If a teacher wants to categorize students for grades A,B,C and D, then they would use 4 clusters. The same algorithm could be applied to network infrastructures. Clusters can be categorized based on normal and abnormal network traffic. Like in the first example, K represents grades, in this scenario K separates normal traffic flow from abnormal traffic flow. This data can be analyzed through a graph. The figure below demonstrates basic k means clustering, and how it can be applied to a network scenario.

The AWS platform and Azure platform also provide a similar online dashboard, including the same and better resources for detecting security threats over the network. In my opinion, for APT 1, the AWS cloud platform should be used in conjunction with Splunk to obtain a zero-trust security posture. Within the AWS platform, hundreds of applications are available that are tailored to specific network needs and industry needs. One of the most significant tools in AWS to detect threats with machine learning is Amazon GuardDuty, its main attribute is to continuously monitor for compromised accounts, and anomalies within the network and end devices. It uses all the resources it has to detect such activity before identifying the severity of the threat with machine learning. It then creates an alert for an end user or administrator to analyze the findings. Although this seems like a long process, GuardDuty can be used to identify threats or anomalies in real-time. Alerting network administrators as fast as possible.

Another reason why GuardDuty can be significant for identifying APT 1 threat actors is because of their use of stolen credentials for VPN's. They will use this method to disguise themselves as employees when gaining access to AWS resources and trying to escalate privileges. GuardDuty will be able to identify if two or more users in different locations are using an employee's VPN, an alert will be created, and

investigation and mitigation actions will take place. In the figure below documentation from AWS provides a visual graphic on how AWS GuardDuty works.

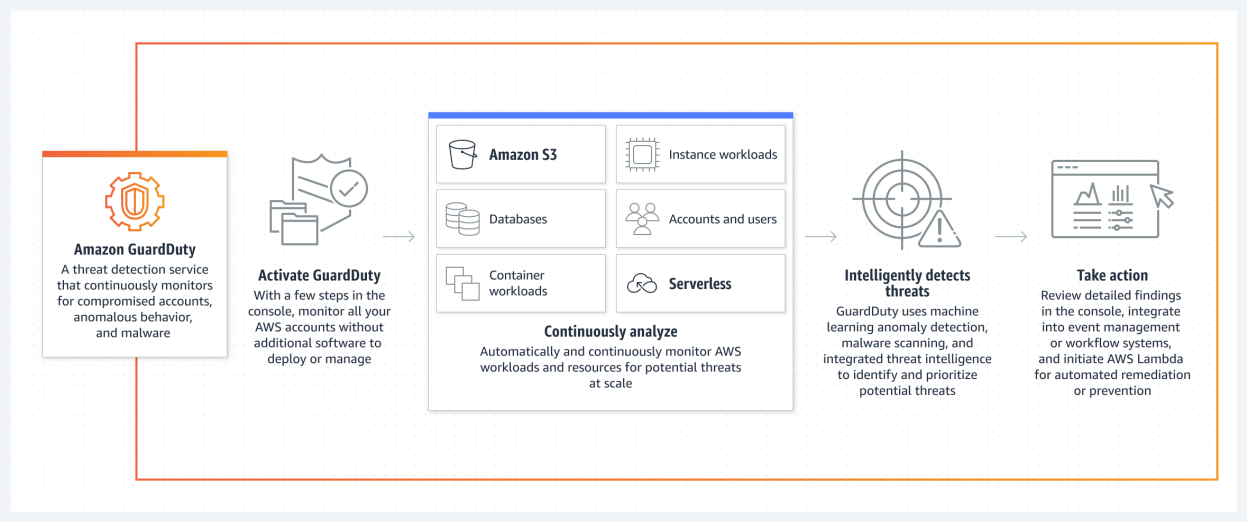

Figure 6: Amazon GuardDuty visual graphic - Steps it takes to identify and stop threats using continuous analysis and machine learning.

Furthermore, Natural Language Proccessing (NLP) can also be a very useful tool for identifying APT 1 threat actors. In Mandiant's report, recuirtment to APT 1 required some profeciency in English. However, there are some documented English statements that are grammicatlly incorrect in APT 1's malware family. For example: 'File no exist' 'Shell is not exist or stopped' 'the url no respon!' 'Doesn't Started!' are evident examples that the malware APT 1 uses doesn't hold English profiency to a high degree.

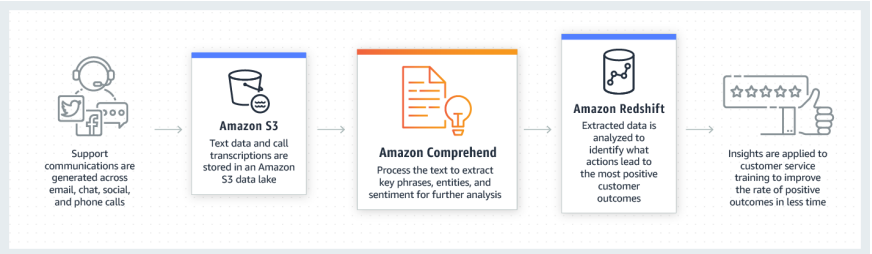

Figure 7:How Amazon Comprehend Works – How it can be used for network security purposes

Amazon Comprehend is usually seen as a tool to retrieve sentiment analysis for buisnesses, and create a more successful organization within an industry. However, Amazon Comprehend can also be used to detect the example anomalies, by storing all communication in a storage lake (a reposository for large amounts of data.) Amazon Comprehend then analyzes all the data and categorizes them. APT 1 communications can be detected in a faster process when using Amazon Comprehend. Once the communications are categorized, administrators will see the difference between regular employee communication vs. APT 1 threat actor communication (if they exist in the network infrastructure.) From here, steps should be used to isolate the compromised account(s), deleting the user(s) from the organization and informing employees about credential theft by APT 1.

Part 6: Ethics in Cybersecurity

More often today, the conversation of ethics has continued to carry the conversation. It is reasonable to question if intentional targeting of security gaps relay to ethical failures by security teams. However, it is important to understand the level of complexity of the threat, as well as standardized security practices vs what is recommended. Since many initial exploitations performed by APT 1 often use Zero-days or Spear Phishing, it can be challenging for security professionals to defend against. As threats continue to advance, it's vital to understand comprise and vulnerability will always be an ongoing challenge that should be viewed as an one size fits all approach. Understanding how APT 1 operates specifically is important. The threat actor aims to cause significant harm to both privacy and property within the targeted networks infrastructure and devices. When discussed in correlation to the C-I-A triad, the APTs goals directedly impacts each of the pillars.

Confidentiality: APT 1 solely works to steal Intellectual Property in addition to other sensitive data. This will directly diminish any types of competitive advantage from having the data leaked.

Integrity: APT 1's aim at stealing data directly gives them the opportunity to manipulate or corrupt it which directly causes concern for the trustability within the information.

Availability: APT 1 is not known to impact system uptime since their goal is to obtain the largest amount of dwell time on a network without being detected.

In general, many companies don't publicly share when they are breached which is concerning from the security perspective. As security professionals this can be perceived as unethical simply because known information is being withheld that may directly be relatable to other investigations. However, understanding how fear can easily make things worse, it is understandable to believe withholding the information is for the greater good. This is primarily because the amount of cyber-attacks that occur on a daily may but our country into a state of panic. Nevertheless, at minimum, organizations that provide goods, resources, or services to the general public should still be required to maintain an obligation to transparently disclosing security breaches to protect customers from ongoing cyber threats.

Conclusion

In many instances, vulnerabilities targeted by APT1 often times originated from a variety of obstacles common within cybersecurity. This Cyber Security Threat Landscape write up has demonstrated the growing sophistication, complexity, and persistence of state sponsored malicious cyber actors by specifically focusing on common tradecraft used by APT 1. There demonstration of advanced Spear-phishing campaigns, customized malware, remote access tooling, and exploitation of zero day vulnerabilities have proved them to be a serious threat to information systems nationally. They are an elite example of what the modern cyber threat landscape resembles in many cases surrounding nation-state level cyber espionage. It is imperative that security professionals continue to pursue newer methods of collection, information sharing, detection and response.

References

Amazon Web Services. (2024). *Amazon GuardDuty*. AWS. https://aws.amazon.com/guardduty/

APT1: Exposing one of China's cyber espionage units. (n.d.-a). https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

APT1. (2021, May 31). APT1. APT1, Comment Crew, Comment Group, Comment Panda, Group G0006 | MITRE ATT&CK®. https://attack.mitre.org/groups/G0006/

Gray, C. (2021, November 16). Top 10 AI-enabled cyber security companies. AIMagazine. Retrieved September 22, 2024, from https://aimagazine.com/technology/top-10-ai-enabled-cyber-security-companies

History of cybersecurity: How it started, and how it's changed | Lucidum ®. (n.d.). https://lucidum.io/blog/history-of-cybersecurity-how-it-started-and-how-its-changed/

Infinity, A. (2024, July 9). Shocking insights and truths about APT1 that DND and CAF may not know. Medium. https://medium.com/aardvark-infinity/shocking-insights-and-truths-about-apt1-that-dnd-and-caf-may-not-know-210c5737ef07

Khan, S. (2024, August 7). APT1 China's Cyber Espionage Group attack life cycle with reference to mandiant attack cycle. Medium. https://securitywithblue.medium.com/apt1-chinas-cyber-espionage-group-attack-life-cycle-with-reference-to-mandiant-attack-cycle-4a8638a7d66a

Matt. (2020, January 15). APT1 and learning from their OPSEC FAILURES. osintme.com. https://www.osintme.com/index.php/2020/01/15/apt1-and-learning-from-their-opsec-failures/

Nation-state cyber actors. Nation-State Cyber Actors | Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors#:~:text=APT%20actors%20are%20well%2Dresourced,network%2Fsystem%20disruption%20or%20destruction.

Slideshare. (2009, April 26). *Ironport Data Loss Prevention*. SlideShare. https://www.slideshare.net/slideshow/ironport-data-loss-prevention251108/1343048#6

Snort 3 rule writing guide. Snort 3 Rule Writing Guide - Snort 3 Rule Writing Guide. (n.d.). https://docs.snort.org/

Staff, C. (2024, March 19). What is data analytics? Key concepts, skills, and careers. Coursera. Retrieved September 22, 2024, from https://www.coursera.org/in/articles/data-analytics

SWAIN, S. (2023, March 2). "Exposed: The activities of APT1, China's notorious Cyber Espionage group". LinkedIn. https://www.linkedin.com/pulse/exposed-activities-apt1-chinas-notorious-cyber-espionage-swain

Waterhouse, S. (2024, June 24). Unmasking APT1: Inside the operations of China's Premier Cyber Espionage Group. LinkedIn. https://www.linkedin.com/pulse/unmasking-apt1-inside-operations-chinas-premier-cyber-steve-jdqwc

What is machine Learning? Definition, types, and examples. | CQF. (n.d.). Certificate in Quantitative Finance. Retrieved September 23, 2024, from https://www.cqf.com/blog/what-machine-learning-definition-types-and-examples?gad_source=1

Yasar, K. (2023, December 7). What is an advanced persistent threat (APT)?: Definition from TechTarget. Security. https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT