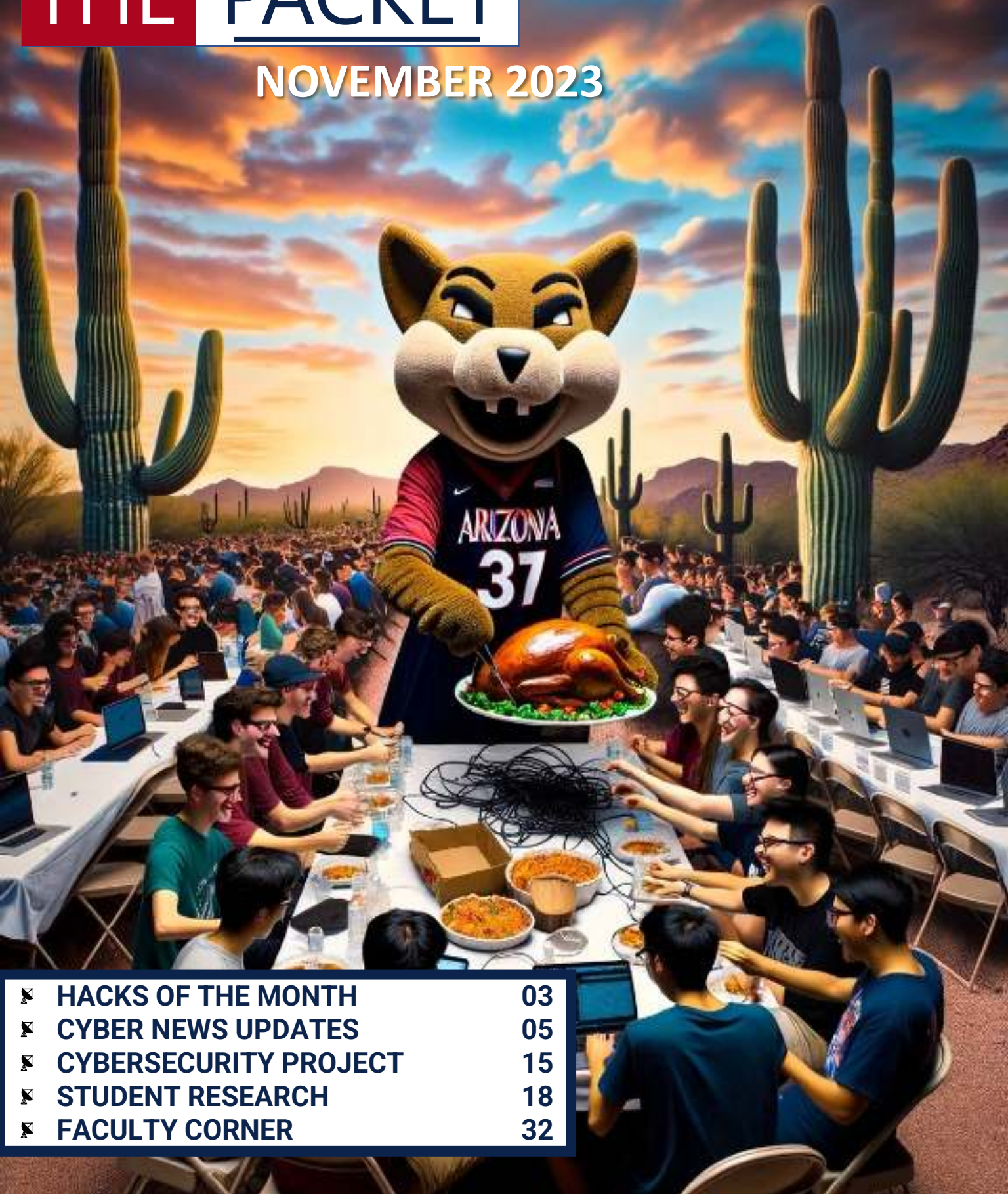


THE PACKET

NOVEMBER 2023



✦ HACKS OF THE MONTH	03
✦ CYBER NEWS UPDATES	05
✦ CYBERSECURITY PROJECT	15
✦ STUDENT RESEARCH	18
✦ FACULTY CORNER	32



New FAFSA Update

October 2023

By now, you've likely heard that the Free Application for Federal Student Aid (FAFSA) is getting an update. We are busy learning about all of the changes and want to make sure we keep you in the loop.

For now, here are the top three things we are sharing with students about the new FAFSA:

The FAFSA usually opens every year on October 1st, but with this update, there will be a delay.

The 2024/2025 FAFSA is scheduled to open sometime in December 2023, no later than January 1, 2024.

Our FAFSA Priority Filing Date will remain March 1st for current students and April 1st for incoming students.

In the coming months, we'll be updating our website and sending short, timely emails, to make sure we are all prepared for the launch of the new FAFSA.

Some things to look forward to include:

- information regarding the FSA ID
- use of Federal Tax Information (FTI)
- who is a "Contributor" and how this may impact the work you do with students

We are grateful to have partners like you across our campus and community who are dedicated to ensuring our students have the tools they need to be successful.

Thank you,
Office of Scholarships and Financial Aid

From Shadows to Spotlight: Iran's MuddyWater Group Strikes Again

MuddyWater, an Iranian state-aligned advanced persistent threat (APT) group, has been actively spying on an unnamed Middle Eastern government for eight months. The group is also known by various other names, such as APT34, Crambus, Helix Kitten, and OilRig.

- The campaign initiated on Feb. 1 with an unknown PowerShell script from a suspicious directory.
- MuddyWater employed four custom malware tools in its campaign, three of which were unfamiliar to cybersecurity experts. These include:
 - Backdoor.Tokel: Downloads files and executes arbitrary PowerShell commands.
 - Trojan.Dirps: Used for PowerShell commands and enumerates files in a directory.
 - Infostealer.Clipog: Capable of keylogging, logging processes for keystrokes, and copying clipboard data.
 - Backdoor.PowerExchange: This PowerShell tool logs into Microsoft Exchange Servers using hardcoded credentials for command-and-control and monitors emails sent by attackers.
- In addition to custom tools, MuddyWater also leveraged two popular open-source hacking tools: Mimikatz and Plink.

The group's success in evading detection for months can be credited to its choice of tools. Introducing new tools and using legitimate ones does not raise immediate suspicions, making detection challenging.

Ransomware Surge: AvosLocker Targets Essential US Sectors Amidst Global Increase

In a combined security advisory, the Cybersecurity Infrastructure and Security Agency (CISA) and the FBI indicated that AvosLocker has been targeting multiple vital sectors in the US, with instances noted as recent as May. The group employs a diverse range of tactics, techniques, and procedures (TTPs), such as double extortion and utilizing trusted native and open-source software. This advisory comes amid a rising trend of ransomware attacks across various sectors. A report by the cyber-insurance company, Corvus, disclosed a nearly 80% surge in such attacks compared to the previous year. Furthermore, there was a growth of over 5% in ransomware activity in September alone. Organizations are urged to take immediate preventive steps. Ryan Bell highlights the pattern of ransomware groups becoming more active after summer. He pointed out the uptick in ransomware attacks in September as an early warning sign and anticipates a rise in attacks in the fourth quarter, based on trends from 2022 and 2021.



Behind the Breach: Sandworm's Exploitation of Ukrainian Telecom Vulnerabilities

The state-sponsored Russian hacking group Sandworm compromised 11 Ukrainian telecommunication providers between May and September 2023. The Ukrainian Computer Emergency Response Team (CERT-UA) reported these breaches, noting service interruptions and potential data breaches caused by the hackers.

Sandworm, linked to Russia's GRU (armed forces), utilized tactics such as phishing, Android malware, and data-wipers throughout 2023. The attack began with network reconnaissance using the 'masscan' tool. Sandworm targeted open ports and unprotected RDP or SSH interfaces. Other tools like 'ffuf', 'dirbuster', 'gowitness', and 'nmap' were used to identify web service vulnerabilities. The hackers exploited VPN accounts without multi-factor authentication and used proxy servers like 'Dante' and 'socks5' to conceal their activities. Two backdoors, 'Poemgate' and 'Poseidon', were identified in the breached systems. While 'Poemgate' captures admin credentials, 'Poseidon' offers extensive remote-control capabilities and maintains its presence by modifying Cron. Sandworm employed the 'Whitecat' tool to remove evidence and deployed scripts to disrupt services, especially targeting Mikrotik equipment.



Octo Tempest: Microsoft Exposes a Formidable Financial Cyber Threat

Microsoft has unveiled an in-depth analysis of "Octo Tempest", a native English-speaking cybercriminal group known for its advanced social engineering and ransomware attacks. The group's modus operandi has evolved since 2022, starting with SIM swapping and account theft, especially targeting cryptocurrency holders. By late 2022, their tactics expanded to phishing, massive password resets, and data theft, impacting sectors like gaming, hospitality, retail, and more.

Upon partnering with the ALPHV/BlackCat ransomware group, Octo Tempest began deploying ransomware to both steal and encrypt data. Their tactics include mimicking speech patterns to deceive technical admins, leading to unauthorized password resets and MFA manipulations. Initial access strategies range from SMS phishing, SIM-swapping, and even direct threats of violence. Once inside, they map out the company's digital landscape, escalate privileges, and maintain access by targeting security personnel and disabling security features.

The group uses a myriad of tools, including open-source applications and Azure-based methods, to achieve their objectives. Detecting them is challenging due to their sophisticated techniques, but Microsoft recommends monitoring identity-related processes and Azure environments as a starting point. Octo Tempest primarily seeks financial gain through methods like cryptocurrency theft, data extortion, and ransom demands.





From Pyongyang with Code:

The Evolving Threat Landscape of North Korean APTs

From Pyongyang with Code: The Evolving Threat Landscape of North Korean APTs

North Korean Advanced Persistent Threat (APT) groups have seen unprecedented collaboration since the onset of the COVID-19 pandemic, introducing a new layer of complexity in their cyber operations. Historically distinct groups, such as the **Lazarus Group** and **Kimsuky**, increasingly share tools, information, and efforts, blurring lines of individual operations. This has resulted in diversifying attack methods, including malware tailored for different platforms and potential supply chain risks.

While their operations become more complex, their primary objectives of gathering intelligence and funding the North Korean regime remain consistent. The pandemic-induced challenges, like closed borders, have inadvertently forced increased communication and coordination among these groups.

Increased Complexity - The Shifting Terrain of North Korean Cyber Threats

In the ever-evolving landscape of cyber threats, adaptability is a consistent theme. Yet, the transformative strategies North Korean (APT) groups adopted recently have added unprecedented intricacy, challenging global defensive frameworks like never before.

Historic Standalone Operations:

In the past, North Korean APTs functioned as isolated units, each characterized by its set of tactics, techniques, and procedures (TTPs). Such demarcation enabled cybersecurity experts to detect, attribute, and neutralize threats based on familiar operational footprints.

Pandemic-Induced Collaborative Dynamics:

The COVID-19 pandemic brought about a pivotal shift in these groups' strategies. Spurred by the pandemic's constraints or strategic recalibration, a pronounced trend towards inter-group collaboration emerged. This unity has birthed a generation of cyber threats that are diverse in their approach and agile in execution.

Blended Operational Tactics:

The era of collaboration witnessed APTs pooling their tools, expertise, and intelligence. This convergence diluted the once-clear demarcations of their operations. Now, an attack might fuse the advanced malware capabilities of one faction with the covert penetration techniques of another, resulting in composite threats that are more challenging to foresee and neutralize.



From Pyongyang with Code: The Evolving Threat Landscape of North Korean APTs

Broadened Attack Spectrum:

This era of shared resources and knowledge has empowered these APTs to cast a wider net concerning their targets. While certain groups once predominantly zeroed in on financial sectors, the collective resource pooling now enables them to launch simultaneous assaults on varied sectors, from energy and healthcare to crucial infrastructures. Moreover, crafting malware designed for diverse platforms, including Windows, Linux, and MacOS, signifies an ambition to capitalize on an expansive set of vulnerabilities.

Operational Confluence:

This newfound collaborative spirit has also seen APTs' operations overlap. It's becoming increasingly typical to observe multiple North Korean APTs converging on a singular target, albeit through varied methodologies. Such a multi-faceted approach can be daunting for defenders, necessitating concurrently responding to various threats.

The intricate nature of the operations of North Korean APTs accentuates the imperative for fluid and forward-thinking defense strategies. As these groups persistently refine their collaborative efforts and resource-sharing, the onus is on defenders to similarly evolve, embracing a comprehensive and proactive stance on cybersecurity.

Attribution Challenges - Deciphering the Hand Behind the Cyber Sword

In the realm of cybersecurity, attribution—the act of identifying and linking a cyber attack to a specific actor or group—is of paramount importance. It informs diplomatic, legal, and military responses and deters potential adversaries. However, the evolving landscape of North Korean (APTs) has made this task increasingly labyrinthine.

Historical Clarity:

Historically, the distinct modus operandi, tactics, techniques, and procedures of individual North Korean APTs provided a semblance of clarity. Each group left behind a unique digital "fingerprint," enabling cyber experts to attribute attacks with a reasonable degree of confidence.

The Blurring of Lines:

This clarity has begun to diminish with increased collaboration among North Korean APTs. Shared tools, resources, and tactics have muddied the waters. Attacks today may bear the hallmark techniques of multiple groups, making it arduous to pinpoint responsibility to a singular entity.

From Pyongyang with Code: The Evolving Threat Landscape of North Korean APTs

Shared Malware Repositories and Code:

The sharing of malware codes and repositories among APTs exacerbates the attribution challenge. When multiple groups deploy the same malware strain or exploit, linking an attack to a specific group becomes a complex puzzle.

Use of False Flags:

To further complicate matters, there's the tactic of "false flags," where threat actors deliberately imitate the TTPs of another group to mislead investigators. Given the intermingled operations of North Korean APTs, discerning genuine patterns from deliberate misdirection becomes even more challenging.

Operational Overlaps:

As highlighted in the complexity section, multiple North Korean APTs may target the same entity using varied approaches. This convergence not only poses defensive challenges but also complicates attribution. Analysts must dissect each thread when faced with multifaceted attacks, discerning whether they originate from a single source or multiple collaborating entities.

Global Implications:

The inability to accurately attribute cyber attacks can have significant geopolitical implications. Wrongful attribution can lead to misguided diplomatic or retaliatory actions, potentially escalating tensions.

Attribution is no longer a straightforward endeavor in the context of North Korean APTs. The intertwined operations shared resources, and deliberate obfuscations demand reevaluating traditional attribution methodologies. Cybersecurity experts must now employ a combination of technical forensics, human intelligence, and geopolitical analysis to discern the puppeteers behind the digital curtains.

Supply Chain Risks - North Korean APTs' Expanding Attack Surface

With their vast and interconnected nature, supply chains have always been prime targets for cyber adversaries. Their multifaceted structure provides numerous infiltration points, and successful breaches can have cascading effects. North Korean APTs, recognizing this potential, have increasingly targeted supply chains, introducing a plethora of risks that need urgent attention.

From Pyongyang with Code: The Evolving Threat Landscape of North Korean APTs

The Allure of the Supply Chain:

Supply chains, by design, involve multiple entities—manufacturers, suppliers, distributors, and customers. Each entity can have its cybersecurity practices, creating a myriad of vulnerabilities. This presents a 'domino effect' opportunity for threat actors: compromise one weak link, and you gain the potential to affect all others in the chain.

Historical Precedence:

While supply chain attacks aren't entirely novel, their frequency, sophistication, and scale have seen a marked increase with the collaborative evolution of North Korean APTs. Their ability to pool resources, share intelligence, and coordinate attacks makes them especially formidable adversaries in the context of supply chain threats.

Tactical Shifts:

Traditionally, many cyberattacks focused on end targets—breaching a specific organization or entity. However, North Korean APTs, recognizing the leverage supply chains offer, have shifted some of their focus. By targeting software providers, third-party vendors, or even logistics partners, they can potentially gain access to a much broader set of final targets.

Real-World Implications:

The ramifications of supply chain attacks can be widespread. They can lead to intellectual property theft, disruption of critical services, financial losses, and even potential physical damages if industrial control systems are involved. For businesses, this also translates to reputational damage and possible legal consequences.

Necessity of Collaboration -Countering North Korean Through Unified Efforts

In an era where threats are increasingly sophisticated and borders in the digital realm become nebulous, collaboration emerges as a potent weapon. As North Korean APTs band together, refining their tactics and pooling resources, the need for collaborative defense strategies among nations and organizations has never been more paramount.

Mimicking the Adversary:

The adage "Know your enemy" is a timeless piece of wisdom. North Korean APTs have demonstrated the power of collaboration, with their combined efforts leading to more intricate, adaptable, and potent cyber threats. To counteract this, defenders must adopt a similar collaborative ethos, sharing intelligence, resources, and strategies.

From Pyongyang with Code: The Evolving Threat Landscape of North Korean APTs

Breaking Silos in Cyber Defense:

Traditionally, nations, organizations, and sectors have operated in silos, guarding their cyber intelligence and defense tactics. However, in the face of a unified threat, such isolated strategies can be counterproductive. Collaboration fosters a dynamic where one entity's detection of a novel threat or tactic can be rapidly disseminated, shielding others from potential breaches.

The Power of Collective Intelligence:

When multiple entities collaborate, they pool not just resources but also intelligence. This collective intelligence—encompassing diverse data points from varied sectors, regions, and systems—creates a more comprehensive view of the threat landscape. It allows for quicker identification of patterns, faster mitigation of threats, and a proactive approach to emerging vulnerabilities.

Overcoming Geopolitical Barriers:

While the digital realm offers seamless connectivity, geopolitical barriers often hinder collaboration. Trust deficits, strategic interests, and historical animosities can deter nations and organizations from sharing vital cyber intelligence. Overcoming these barriers is crucial. The shared threat of North Korean APTs offers an opportunity for entities to prioritize collective security over individual interests.

Frameworks and Platforms:

For collaboration to be effective, structured frameworks and platforms are essential. These can facilitate real-time sharing of threat intelligence, coordination of defense strategies, and joint research endeavors. Through intergovernmental alliances, industry consortiums, or public-private partnerships, such collaborative platforms can amplify the collective defense capabilities. The evolving tactics of North Korean APTs underline a pressing reality: the old paradigms of isolated cyber defense are inadequate. In a world where threat actors continually innovate and collaborate, defenders must reciprocate in kind. The necessity of collaboration isn't just a strategic choice; it's an imperative for global cyber resilience.



From Pyongyang with Code: The Evolving Threat Landscape of North Korean APTs

Why Would North Korea Have Multiple APT Groups?

Specialization:

Each APT group can specialize in a specific type of cyber operation. Some groups might focus on intelligence gathering, others on financial theft, and yet others on creating disruptions. By specializing, each group can develop deep expertise in its area, leading to more successful operations. For instance, the Lazarus Group is known for its aggressive financial theft operations, while APT37 (or Reaper) is more focused on espionage against specific targets.

Compartmentalization:

In intelligence and military operations, compartmentalization is a standard procedure. By keeping operations and groups separate, the compromise of one group doesn't necessarily jeopardize others. If one group is detected or its methods are exposed, other groups can continue their operations unaffected.

Diversification of Tactics:

Different groups can employ varied tactics, techniques, and procedures (TTPs). This diversification makes it harder for defenders to predict and counter threats. When facing multiple groups with different TTPs, defenders must spread their resources and attention, making their defense posture potentially weaker.

Geopolitical Strategy:

By maintaining multiple APT groups, North Korea can pursue different geopolitical objectives simultaneously. One group might target institutions in a rival country, and another might focus on gathering intelligence from international organizations. Yet, another might focus on stealing funds to bypass economic sanctions.

Redundancy:

In cyber operations, redundancy can be beneficial. If one group faces setbacks or its operations are thwarted, others can take over or ramp up their activities. This ensures continuous pressure on targets and maintains the momentum of cyber campaigns.

Deception and Misdirection:

Multiple groups can engage in "false flag" operations, where they deliberately imitate the TTPs of other groups, confusing defenders and making attribution more challenging. This can lead to misdirected blame, creating geopolitical tensions elsewhere while the actual perpetrator remains obscured.

From Pyongyang with Code: The Evolving Threat Landscape of North Korean APTs

Evolution and Adaptation:

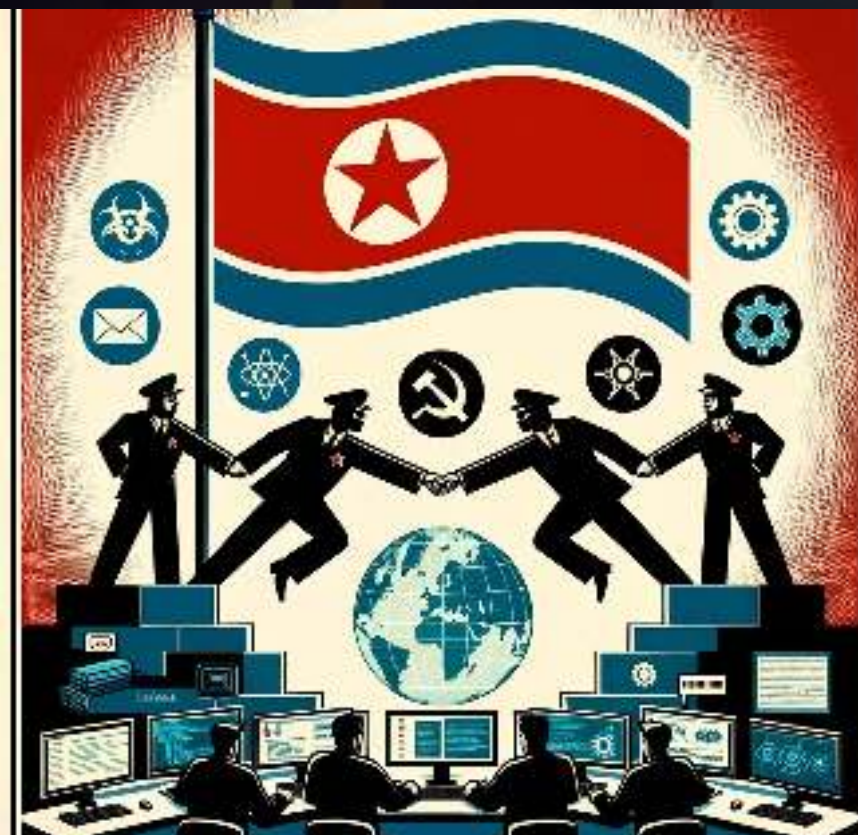
The cyber realm is dynamic, with rapid technological advancements. Multiple groups allow for parallel evolution and adaptation. As one group learns and innovates, it can share its advancements with others, ensuring that the nation's cyber capabilities are continually refined.

Having multiple APT groups provides North Korea with flexibility, a diversified approach, and a multi-pronged strategy in its cyber operations. It allows for a combination of specialization and broad coverage, ensuring that the nation can pursue its objectives effectively in the cyber domain.

The evolving landscape of North Korean (APT) groups presents new challenges in cybersecurity. These groups, once distinct in their operations, are now collaborating more than ever, increasing their effectiveness and complicating defense efforts.

Their shift towards shared resources and tactics has made attribution difficult. Furthermore, their expanded focus on supply chain vulnerabilities has broadened the potential attack surface. This change in strategy necessitates a parallel shift in defense approaches.

However, there's an evident solution: collaboration. Just as North Korean APTs have united, global defenders must also come together. Sharing intelligence and resources could be the key to countering these collective threats. As the cyber landscape changes, so too must the strategies to defend it.



Want to learn more about US & China relations?

Join us for the first panel discussion

CAST DISTINGUISHED SPEAKER SERIES **CAST**

November 7th · 2pm · Hybrid Event

PANEL:

Dr. Bill Cassidy - Senior United States Senator for Louisiana

Dr. Daniel C. Tirone- Associate Professor of Political Science at Louisiana State University (attending virtually)

REGISTER TODAY!



College of Applied
Science & Technology

CAST

DISTINGUISHED SPEAKER SERIES

2023-2024 Theme:

CURRENT ISSUES IN NATIONAL AND INTERNATIONAL SECURITY

Nov. 7 Panel Discussion: The US & China

2pm

Scheduled guest panelist: U.S. Senator William Cassidy of Louisiana (attending virtually) and Dr Daniel C. Tirone Associate Professor of Political Science at Louisiana State University (virtually)

Feb. 29 Reflections on Cybersecurity and National Security

4:30-
6:30

Talk on the current state and future developments in Cybersecurity by Chet Hosmer, Professor Emeritus of Cyber Operations, College of Applied Science and Technology, author of seven books, and internationally recognized leader in cybersecurity.

April 11 Panel Discussion: The US, Europe & Russia

4:30-
6:30

Panel moderated by Dr. Nic Rae, Professor of Government and Public Service and Associate Dean for Research, College of Applied Science and Technology. Our panelists are Dr. Paul J. D'Anieri Professor of Political Science and Public Policy from University of California Riverside and Dr. Dmitriy Nullurayev, Assistant Professor of Government and Public Service, College of Applied Science and Technology

SPONSORED BY:



[Register](#) >

Introducing HexCheck: A Python Network Visualization Tool

HexCheck is a Python-based network visualization tool that utilizes the Tkinter library for its graphical interface. It's designed to visually represent the status of various network hosts and services, using color-coded hexagons on a canvas. Each hexagon represents a service, with its color indicating the service's status: red for an unreachable host, green for a responsive service, and blue for a reachable host with a closed port.

Code Breakdown:

Importing Libraries

The script begins by importing the necessary libraries:

- **tkinter**: for the GUI.
- **subprocess**: to execute shell commands.
- **socket**: for network connections.
- **platform**: to determine the operating system.
- **os**: to interact with the operating system.
- **time**: to handle time-related tasks.

```
1 import tkinter as tk
2 import subprocess
3 import socket
4 import platform
5 import os
6 import time
7
```

Utility Functions

- **is_host_alive(ip)**: Checks if a host is alive by pinging its IP address.
- **is_port_open(ip, port, timeout=1)**: Checks if a specific port on the host is open.
- **get_hexagon_status_color(ip, port)**: Returns a color based on the status of the host and port.

Drawing Functions

- **draw_hexagon(canvas, x, y, size, fill_color, name)**: Draws a hexagon on the canvas.
- **update_hexagon_color(x, y, size, fill_color, canvas_item)**: Updates the color of an existing hexagon on the canvas.
- **draw_all_hexagons(canvas, servers)**: Draws all the hexagons based on the configuration.

Introducing HexCheck: A Python Network Visualization Tool

Configuration Parsing

- `parse_config(filename)`: Reads server information from a configuration file, falling back to a default configuration if the file doesn't exist.

Canvas and GUI Functions

- `update_canvas()`: Updates the canvas by changing the color of hexagons to reflect the current status of each server.
- `adjust_canvas_size(canvas, servers)`: Adjusts the canvas size to fit all hexagons based on the number of servers.
- `toggle_fullscreen(event=None)`: Toggles fullscreen mode for the application.
- `create_context_menu(event)`: Creates a right-click context menu with options like toggling fullscreen and exiting the application.

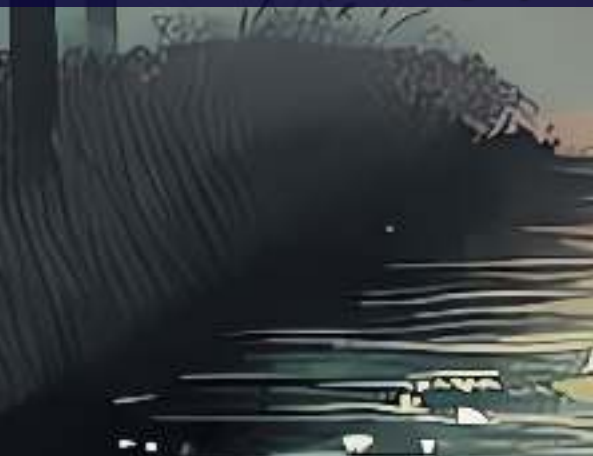
Main GUI Setup

The main part of the script sets up the GUI window, binds events, creates a context menu, parses the configuration file, and starts the main loop.

Setting Up HexCheck:

To set up HexCheck, follow these steps:

1. Ensure you have **Python** installed on your system.
2. Install the **Tkinter** library if it's not already available.
3. Save the HexCheck code to a file, for example, **hexcheck.py**.
4. Create a **config.txt** file with your server information or allow the script to generate a default one for you.
5. Run the script using Python: **python hexcheck.py**.

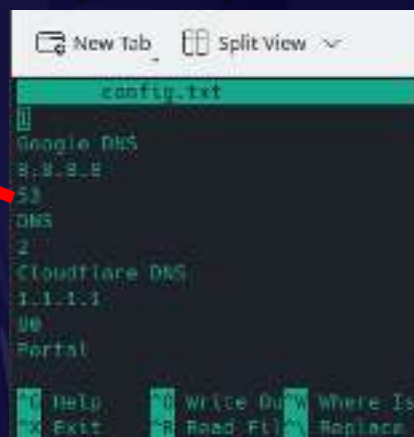


Introducing HexCheck: A Python Network Visualization Tool

Community Engagement:

For students or other individuals who are interested in contributing to HexCheck, you are encouraged to fork the repository where HexCheck is hosted. Once forked, you can modify the code, add features, or fix any issues you may encounter. Active participation in such projects can be an excellent way to learn more about Python, network programming, and open-source collaboration.

```
# Entity Number
# Name of Service
# IPv4 Address
# Service Name
# Service Port to check
```



```
config.txt
Google DNS
8.8.8.8
53
DNS
2
Cloudflare DNS
1.1.1.1
44
Portal
```

Setting Up config.txt:

To set up your config.txt file, follow these steps:

1. **Create the File:** Start by creating a plain text file named **config.txt** in the same directory as your HexCheck script.
2. **Add Server Details:** Within this file, add the details of each server you want to monitor. Follow the structure outlined above, ensuring that each server's details occupy exactly five lines.
3. **Repeat for Additional Servers:** If you have more than one server to monitor, repeat the five-line block for each one, incrementing the identifier for each new server.
4. **Save the File:** After adding all the necessary server details, save the **config.txt** file.

If the config.txt file does not exist when you run HexCheck, the script is designed to create a **default config.txt** file with a pre-defined configuration. You can then modify this file with your own server details as needed.

Conclusion:

HexCheck serves as a practical tool for network administrators and students alike to monitor network services visually. Its simplicity and the use of a graphical interface make it an excellent project for those looking to delve into the intersection of networking and programming.

Covert Communications in Network Protocols: A Study of Techniques

By: Kiran Raavi

This research paper explores the realm of network-based covert communications and data hiding, focusing on three prominent techniques: TCP/IP Steganography, Covert Timing Channel Steganography, and DNS Tunneling. These methods operate discreetly within network traffic, concealing sensitive information and enabling covert communication. Through in-depth analysis, we unveil their principles, applications, and the emerging synergy between DNS Tunneling and network steganography.

Introduction:

Covert communications and data hiding, known as steganography, have transcended ancient practices to find a home within computer networks. This paper ventures into the intricacies of network-based covert communications and steganography, illuminating the methods by which information is concealed within the vast labyrinth of digital communication. As we delve into this secretive domain, we aim to distinguish network-based steganography from its counterparts. Unlike traditional steganography, which embeds data within static media such as images or audio, network-based steganography conceals information within the dynamic flow of network traffic. This distinction provides attackers with a potent tool, allowing them to establish covert communication channels that operate under the radar of traditional security measures. These covert channels are of paramount importance to attackers. They serve as conduits for transmitting sensitive information, evading detection, and achieving their nefarious objectives. From espionage to data exfiltration, cyber-espionage, and censorship circumvention, these channels offer a cloak of invisibility in the digital realm. In this paper we will dissect three network-based covert communications techniques: TCP/IP Steganography; Covert Timing Channel Steganography; and DNS Tunneling. Each method operates within the layered architecture of computer networks, employing unique tactics to hide and extract concealed data. Our journey will encompass detailed analyses, comparative assessments, and a glimpse into the potential of integrating DNS Tunneling with broader network steganography.

TCP/IP Steganography

TCP/IP Steganography is a sophisticated network steganographic technique that operates by concealing data within the packet headers of TCP/IP (Transmission Control Protocol/Internet Protocol) traffic. The technique involves several steps:

- 1. Packet Selection:** The initial step involves the careful selection of specific network packets from an ongoing communication session. These packets are chosen strategically to minimize suspicion and blend in with legitimate traffic.
- 2. Data Embedding:** The core of TCP/IP Steganography lies in the modification of certain fields within the packet headers. These fields are typically chosen to minimize detection, and they commonly include the Time To Live (TTL) field, IP Identification field, and TCP header flags.
- 3. Data Extraction:** On the recipient's side, a complementary algorithm is applied to identify and extract the concealed data from the altered packet headers. This process involves decoding the data and reconstructing the original message [3][4].

Implementation

TCP/IP Steganography can be implemented in various scenarios. In a corporate espionage scenario, an insider can modify the TTL values of ICMP (Internet Control Message Protocol) echo request packets to exfiltrate sensitive data, which is concealed within the TTL field. For covert communication, attackers can use TCP flags to establish a hidden channel within seemingly innocuous web traffic. For instance, they may set specific flag combinations to represent different letters or commands [4].

The Taidoor RAT is a well-documented example of TCP/IP Steganography implementation in the wild. Taidoor used this technique to hide its C2 communications within seemingly legitimate network traffic. It manipulated packet headers to encode and transmit commands to infected systems without raising suspicion. This made it challenging for security systems to detect and block Taidoor's malicious activity [5].

Technical Feasibility

Attackers must possess a deep understanding of network protocols and traffic patterns to manipulate packet headers. Packet header modifications may also introduce errors, potentially corrupting the concealed data. Maintaining data integrity while concealing information adds complexity. The payload capacity of TCP/IP Steganography is contingent on the chosen encoding method and the specific fields within packet headers that are used for data hiding. Bandwidth, in this context, refers to the rate at which data can be covertly transmitted. The capacity may vary depending on the media types used for embedding [3].

When embedding data within the TTL (Time To Live) field, the bandwidth is relatively low. Typically, a binary '0' may be represented by one TTL value, while a '1' corresponds to another value. This binary encoding results in a slower transmission rate due to the limited number of TTL values. Using the IP Identification field for data encoding can provide a slightly higher bandwidth compared to TTL field encoding. This is because the IP Identification field can accommodate a larger range of numerical values, allowing for more efficient data transmission. TCP header flags offer a moderate bandwidth, as there are several flag combinations available to represent binary values. However, this method may be less efficient for transmitting large volumes of data compared to IP Identification field encoding [1][3][4].

Defensive Measures

Detecting TCP/IP Steganography is complex because it requires the ability to differentiate between legitimate and covertly altered packet headers, which can be subtle. It necessitates specialized tools and continuous monitoring for irregular patterns. Detection becomes more feasible with the identification of known signatures or behaviors linked to this technique. DPI (Deep Packet Inspection) tools scrutinize packet headers to identify unusual modifications or anomalies [4]. Anomaly-based IDS can raise alarms when atypical packet header alterations occur, indicating potential steganographic activity [3][4].

Ways to Improve TCP/IP Steganography

- **Encoding:** Encoding can add an additional layer of security against defensive measures. Advanced encoding methods like adaptive encoding, where encoding changes dynamically based on network conditions, can further improve efficiency.
- **Careful selection of packets:** Improving the packet selection process, such as targeting packets with less impact on network performance, can enhance concealment and reduce detection likelihood.
- **Nested Steganography:** Hiding the payload within another carrier can add an additional complexity to hide data from forensic analysis.

Covert Timing Channels

Covert Timing Channels exploit variations in timing, such as packet arrival times or response delays, to convey hidden information. The sender generates a precise timing pattern by introducing controlled delays between network events. These events can include packet transmissions, server responses, or even timing intervals between keystrokes during communication. The introduced delays serve as carriers to encode binary data. For example, a brief delay might signify '0,' while an extended delay indicates '1.' The sender meticulously orchestrates these timing variations to encode the entire message. At the recipient's end, a matching timing pattern is established to extract the concealed data. This is done by carefully analyzing the variations in timing delays and decoding them to reconstruct the original message [6][7].

Implementation

Covert Timing Channels can be implemented in various scenarios. In a botnet operation, attackers can introduce subtle timing variations in their communication with compromised systems. These variations can encode commands or instructions for the compromised bots to execute. A malicious insider can use Covert Timing Channels to exfiltrate sensitive data by introducing timing delays in outgoing network traffic. The delays encode the data, which is then reconstructed at the recipient's end.

"Ping Exfiltration" is a well-known example of Covert Timing Channels. In this technique, attackers manipulate the timing between ICMP echo request

Covert Communications in Network Protocols: A Study of Techniques

By: Kiran Raavi

and reply packets to encode and clandestinely transmit data. By carefully controlling the timing between these packets, they can encode information and transmit it through standard ICMP ping requests and replies [7].

Technical Feasibility

The feasibility of deploying Covert Timing Channels largely hinges on the level of control an attacker can exert over the timing variations within the target network environment. While the concept of manipulating timing intervals to encode data is relatively straightforward, achieving precise and reliable timing control can be challenging. In practice, successful implementation often requires in depth knowledge of the target network's behavior, including its latency characteristics, packet transmission patterns, and response times. This level of insight can be achieved through various means, including reconnaissance and post-exploitation activities. In cases where attackers have a foothold in the network or control over certain network elements, such as routers or servers, they may have an easier time in implementing Covert Timing Channels. However, even in scenarios with limited control, attackers can leverage existing timing variations within protocols or systems to establish covert channels [6][7][8].

The payload capacity is also closely tied to the precision of timing variations achievable within the network. Covert Timing Channels often rely on introducing slight delays between packets or events, with each delay representing a binary '0' or '1'. The bandwidth largely depends on the accuracy of timing control, which can vary from milliseconds to microseconds. The payload capacity is also influenced by the rate at which packets or events occur. Higher packet rates allow for faster data transmission but may risk detection due to more frequent timing variations. Finally, network conditions, such as latency and jitter, can affect the achievable timing precision. More stable and predictable networks may provide a higher payload capacity compared to highly dynamic networks[6][7].

Defensive Measures

Limiting the variability in packet timing can help mitigate covert timing channel attacks. Network traffic can be shaped to adhere to predefined patterns, making it challenging for attackers to introduce noticeable timing variations. Detecting Covert Timing Channels is difficult due to the subtle nature of timing variations. It often requires advanced statistical analysis and specialized monitoring tools for effective identification. These systems analyze timing variations and raise alerts when deviations from expected patterns occur [6][8].

Ways to Improve Covert Timing Channels

Improving the effectiveness of Covert Timing Channels involves several potential strategies:

- **Precise Timing Control:** Implementing more precise timing control mechanisms, such as hardware-based timers, can enhance the accuracy of timing variations and increase the payload capacity.
- **Variable Timing:** Introducing variable timing intervals between events can make the covert channel more challenging to detect. Adaptive timing variations can help mitigate detection based on fixed patterns [7].
- **Compression:** Implementing data compression techniques can optimize data encoding within timing variations, effectively increasing the payload capacity by encoding more information in shorter intervals.
- **Traffic Injection:** Injecting covert timing variations into legitimate network traffic can help mask the channel. This approach relies on leveraging existing traffic patterns to conceal covert communications [7].

Again, the focal point of this technique is the ability to manipulate timing intervals. Any improvement suggestions short of broad TTP combinations must keep this aspect in mind.

TCP/IP Steganography vs. Covert Timing Channels: A Comparative Analysis

The two data hiding methods operate using the same infrastructure, but each offer a unique functionality across several concepts:

- **Payload Capacity:** TCP/IP Steganography offers discrete and relatively low bandwidth for data transmission due to subtle packet header modifications. Covert Timing Channels can potentially achieve higher transmission rates, especially with precise timing control.
- **Detection:** Both techniques are challenging to detect due to their covert nature. Covert Timing Channels may be more resistant to detection when sophisticated timing control is employed, as it can normalize behavior to fool anomaly detection.
- **Technical Feasibility:** TCP/IP Steganography requires deep protocol knowledge but is accessible to attackers with networking expertise. Covert Timing Channels require precise timing control, potentially demanding hardware-level access.
- **Use Cases:** TCP/IP Steganography is better suited for discreet communication, data exfiltration within existing traffic, and bypassing security controls. It also has significant scope to adapt and utilize more specific techniques. Covert Timing Channels excel in scenarios requiring higher data transmission rates and effective control of timing variations.

Ultimately, Covert Timing Channels prioritize potential for higher transmission rates, while TCP/IP steganography tends to maintain focus on discretion and resilience. The choice depends on specific use cases and trade-offs between bandwidth, detection risk, and technical feasibility. Both techniques require ongoing research for effective detection and mitigation.

DNS Tunneling

DNS tunneling is a method of covert communication that capitalizes on the inherent functionality of the Domain Name System (DNS) protocol. It involves embedding data within DNS queries and responses, often using subdomains or resource records.

Covert Communications in Network Protocols: A Study of Techniques

By: Kiran Raavi

The process can be broken down as follows:

- 1. Data Encapsulation:** Data is first divided into smaller, manageable chunks. The size of these chunks can vary depending on the DNS server's configuration and the specific tunneling tool or method used. Each data chunk undergoes encoding to represent it as a valid DNS query or response. Common encoding techniques include Base64, hexadecimal, or binary representations.
- 2. Subdomain or Resource Record Manipulation:** The encoded data chunks are inserted into DNS queries or responses as subdomains or resource records. For example, a subdomain like "sub.domain.com" might be used to carry the encoded data. The choice of subdomains or resource records depends on the tunneling tool and its compatibility with DNS server configurations.
- 3. DNS Server Resolution:** The manipulated DNS queries or responses are sent to a DNS server. These servers are typically either controlled by the attacker (for malicious purposes) or are public DNS servers (for bypassing network restrictions). The DNS server receives these queries or responses and processes them as part of its standard DNS resolution operations.
- 4. Data Extraction:** On the receiving end, a client or a listening component monitors the DNS traffic. This monitoring system extracts the encoded data from the subdomains or resource records. Extracted data chunks are reassembled in the correct order to reconstruct the original message or payload [11].

Implementation

DNS tunneling can serve both legitimate and malicious purposes. It can be used for secure, encrypted communication in scenarios where traditional network traffic may be monitored or restricted. Dnscat2 is a legitimate tool designed for secure DNS tunneling. Security professionals use it to establish covert communication channels for testing and secure data transfer. On the other side, malicious actors employ DNS tunneling for a range of activities, including command and control communication, data exfiltration, and concealing their actions within a network. The banking trojan IcedID has used DNS tunneling to communicate with its C2 servers.

By encapsulating malicious data within DNS queries and responses, it evades traditional network security measures, making it challenging to detect and mitigate [11].

Technical Feasibility

The technical feasibility of deploying DNS tunneling largely depends on the attacker's knowledge and resources. Setting up a basic DNS tunnel is relatively straightforward, but evading detection is a complex and ongoing challenge. In terms of payload capacity of DNS tunneling, it varies based on several factors:

- **DNS Message Size Limit:** The typical DNS message size limit is 512 bytes for UDP queries, which limits the size of each chunk.
- **DNS Server Configuration:** Some DNS servers may impose restrictions on the size of DNS messages, which can limit payload capacity.
- **Encoding Method:** The encoding method used affects the efficiency of data representation. Different encoding techniques result in varying levels of overhead.

Overall, payloads are often limited to a few hundred bytes per query or response, making DNS tunneling suitable for transmitting relatively small amounts of data [11][12].

Defensive Measures

Mitigating DNS tunneling risks can be complex but is critical for network security. Several controls and measures can be implemented:

- **DNS Sinkholing:** DNS sinkholing involves redirecting DNS queries for known malicious domains to a sinkhole server that logs the activity or returns false information. Sinkholing known malicious domains associated with DNS tunneling tools or command and control servers can disrupt tunneling attempts. It effectively halts communication with malicious entities.
- **Deep Packet Inspection (DPI):** DPI involves the inspection of the actual content of network packets, allowing for the detection of anomalies or suspicious patterns. DPI can be a potent tool for identifying DNS tunneling activity by examining the payload of DNS packets. It can detect encoded data that does not conform to expected DNS traffic patterns.

Covert Communications in Network Protocols: A Study of Techniques

By: Kiran Raavi

- **DNS Security Extensions (DNSSEC):** DNSSEC is a suite of extensions that adds an additional layer of security to DNS by digitally signing DNS data. DNSSEC helps verify the authenticity of DNS responses, reducing the risk of DNS tunneling attacks that rely on forged DNS data.
- **Rate Limiting:** Rate limiting restricts the number of DNS queries that can be made in a given time frame. Implementing rate limiting on DNS queries can hinder the efficiency of DNS tunneling attempts, as it limits the volume of data that can be transmitted within a short period [10].

Detection of DNS tunneling can be challenging, especially when encryption is used. Anomaly detection in DNS traffic patterns and monitoring for suspicious subdomains or resource records can provide a wide net. However, sophisticated attackers continuously develop evasion techniques to circumvent detection.

Ways to Improve DNS Tunneling

Improvements to DNS tunneling techniques involve enhancing encryption, obfuscation, and evasion methods. Additionally, the development of more advanced tunneling protocols capable of bypassing increasingly sophisticated detection mechanisms is an ongoing area of research. As we will explore later, there is a lot of potential to combine DNS Tunneling with other techniques to develop a robust set of TTPS.

Comparative Analysis of DNS Tunneling and Network Steganography

DNS tunneling differs fundamentally from network-based steganography in that it uses the DNS protocol specifically to transmit data covertly. DNS tunneling encodes data within DNS queries and responses, often using subdomains or resource records. Network-based steganography, on the other hand, embeds data within the actual network packets themselves. There are a number of aspects across which these techniques offer unique capability.

Visibility

DNS tunneling, by its nature, involves interactions with DNS servers, which can make it more visible at the network level. While it can blend with legitimate DNS traffic, certain anomalies may be detectable in DNS

Covert Communications in Network Protocols: A Study of Techniques

By: Kiran Raavi

query patterns, making it somewhat conspicuous. Network steganography operates at a lower protocol layer and does not directly interact with DNS servers, which allows it to blend more effectively with legitimate network traffic. It typically exhibits a lower level of visibility, making it harder to detect.

Detection:

Detecting DNS tunneling can be challenging due to its ability to mimic legitimate DNS traffic. Detection methods often rely on identifying anomalies in DNS traffic patterns, monitoring for unusual subdomains or resource records, and using Deep Packet Inspection (DPI) techniques. It may require specialized tools and expertise. Detecting network steganography is generally more difficult as it conceals data within the payload of network packets. Specialized tools and algorithms are often needed to distinguish hidden data from normal network communication. Detection relies on identifying patterns or anomalies that deviate from expected network traffic behavior [10].

Payload Capacity:

The payload capacity of DNS tunneling is constrained by DNS message size limits, typically limited to 512 bytes for UDP queries. This limitation restricts the size of each data chunk, making DNS tunneling suitable for transmitting relatively small amounts of data in each query or response. Network steganography's payload capacity is primarily constrained by the size of network packets. It can potentially accommodate larger amounts of data within each packet, depending on the network packet size and the chosen embedding technique. This makes it more suitable for transmitting larger volumes of covert data [2][11].

Covert Communications in Network Protocols: A Study of Techniques

By: Kiran Raavi

Resilience Against Mitigations:

DNS tunneling may be more susceptible to network security mitigations like DNS sinkholing and rate limiting. These measures can disrupt tunneling attempts but may not be foolproof against advanced evasion techniques. Network steganography is designed to blend seamlessly with legitimate network traffic, making it more resilient against traditional network-based mitigations. However, its effectiveness can still be compromised if up against robust anomaly detection.

Use Cases:

DNS tunneling is often employed for C2 communication, data exfiltration, and bypassing network restrictions. It has both legitimate and malicious use cases, with legitimate applications in secure communication. Network steganography is primarily used for concealing data within network traffic to evade surveillance or monitoring. Its applications are more focused on maintaining secrecy and are less commonly associated with C2 communication.

In summary, DNS tunneling relies on the DNS protocol to transmit data covertly and may be more visible due to its interaction with DNS servers. Network steganography conceals data within the content of network packets and is designed to blend in with normal network traffic, making it harder to detect but limited by packet size constraints. Both methods serve the purpose of covert communication but operate at different protocol layers with distinct characteristics.

Combining DNS Tunneling with Network Steganography:

DNS tunneling and network steganography are distinct covert communication techniques, but they can be combined to create a more resilient and sophisticated covert channel. This cooperation allows attackers to leverage the strengths of both methods while mitigating some of their individual weaknesses.

Technical Integration:

A few examples of how these techniques can be combined:

1. **Data Fragmentation:** Data can be divided into smaller chunks and distributed across both DNS queries and network packets. This fragmentation makes it harder to detect and reassemble the complete message [4].
2. **Encryption and Obfuscation:** Encrypting data before embedding it in DNS queries and using steganographic techniques within network packets can add multiple layers of security.
3. **Cover Timing DNS:** Covert Timing Channel steganography can be used to control the timing of DNS queries in a similar manner to what was discussed earlier. By introducing intentional delays or patterns into the timing of DNS queries, adversaries make their covert communication less predictable [6].
4. **Protocol Switching:** Adversaries may employ dynamic communication protocols that switch between DNS tunneling and network steganography based on reconnaissance of network conditions and security measures. This adaptability enhances their resilience against detection.

One notable example of combining DNS tunneling with network steganography is the "Duqu" malware, which is related to the Stuxnet worm. Duqu utilized a multi-stage communication mechanism which integrated both techniques. Duqu initially used DNS tunneling to establish contact with its command and control (C&C) servers. This allowed it to bypass certain network restrictions and evade detection. Once the initial connection was established, Duqu switched to network steganography to further covertly communicate with its C&C servers. It embedded data within seemingly legitimate network packets, making it extremely difficult to distinguish malicious traffic from legitimate traffic. The combination of these techniques made Duqu a highly sophisticated and elusive piece of malware [9].

Advantages of Combining Techniques:

By combining DNS tunneling with network steganography, attackers can make it significantly more challenging for security systems to detect and block their covert communication channels. The use of multiple techniques can help adversaries minimize their digital footprint, making it less likely that security analysts will notice unusual patterns of behavior. Combining methods also allows attackers to adapt to changing network conditions and security measures more effectively.

In summary, the integration of DNS tunneling with network steganography represents a highly advanced and evasive form of covert communication. While it significantly raises the bar for detection and mitigation, it also highlights the importance of comprehensive security measures that encompass both DNS traffic monitoring and network packet analysis.

Conclusion

In the realm of covert communications and data hiding, network protocols offer a vast domain for exploitation. The constant evolution of protocols allows for continuous opportunity to develop data hiding methods which can be increasingly dynamic. This is even more telling in the backdrop of developments in neural networks and AI technologies. Research into this field is more urgent than ever if security practitioners are to stay ahead of the curve of stealthy attackers.

References

1. Lubacz, J., Mazurczyk, W., & Szczypiorski, K. (2014). Principles and Overview of Network Steganography. *IEEE Communications Magazine*, 52(5). <https://doi.org/10.1109/mcom.2014.6815916>
2. Singh, N., Bhardwaj, J., & Raghav, G. (2017). Network Steganography and its Techniques: A Survey. *International Journal of Computer Applications*, 174(2). <https://www.ijcaonline.org/archives/volume174/number2/singh-2017-ijca-915319.pdf>
3. Mileva, A., & Panajotov, B. (2014). Covert Channels in TCP/IP Protocol Stack - Extended Version-. *Open Computer Science*, 4(2). <https://doi.org/10.2478/s13537-014-0205-6>
4. Murdoch, S. J., & Lewis, S. (2005). Embedding Covert Channels into TCP/IP. *Information Hiding*, 247–261. https://doi.org/10.1007/11558859_19
5. Mar-10292089-1.V2 – Chinese Remote Access Trojan: Taidoor: CISA. *Cybersecurity and Infrastructure Security Agency CISA*. (2020, August 3). <https://www.cisa.gov/news-events/analysis-reports/ar20-216a>
6. Cabuk, S., Brodley, C. E., & Shields, C. (2004). IP Covert Timing Channels: Design and Detection. *Proceedings of the 11th ACM Conference on Computer and Communications Security*. <https://doi.org/10.1145/1030083.1030108>
7. Liu, Y., Ghosal, D., Armknecht, F., Sadeghi, A.-R., Schulz, S., & Katzenbeisser, S. (2009). Hide and Seek in Time — Robust Covert Timing Channels. *Computer Security - ESORICS 2009*, 5789. https://link.springer.com/chapter/10.1007/978-3-642-04444-1_8
8. Lu, S., Chen, Z., Fu, G., & Li, Q. (2019). A novel timing-based Network Covert Channel Detection Method. *Journal of Physics: Conference Series*, 1325(1), 012050. <https://doi.org/10.1088/1742-6596/1325/1/012050>
9. Kaspersky Labs (2021, May). The Mystery of Duqu 2.0: A Sophisticated Cyberespionage Actor Returns. *Securelist English Global securelistcom*. <https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/>
10. J. Sunddler, & J. Åstrand. (2019). DNS Tunnelling Detection. Retrieved from <https://www.diva-portal.org/smash/get/diva2:1324289/FULLTEXT01.pdf>
11. Hinchliffe, A. (2019, March 27). DNS tunneling: How DNS can be (ab)used by malicious actors. Unit 42. <https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors>

Managing Data Privacy BY: Professor Jordan A. VanHoy

Loss of Control

In May 2023, one of the largest fines ever imposed for violations of the European Union's General Data Protection Regulation (GDPR) came to light. A historic penalty of 1.2 billion euros was levied against the United States technology giant Meta (Data Privacy Manager, 2023). Known for its popular platforms, including Facebook, Instagram, and WhatsApp, the technology giant failed to adequately protect the data of EU citizens during a transfer from the EU to the US. The initial enforcement action was taken by the Irish Data Protection Commission (DPC), which alleged that Meta, in relying on Standard Contractual Clauses (SCC) and additional administrative controls, did not comprehensively address the risks to data subjects' rights and freedoms. The management of privacy is more of an art than a science, characterized by ambiguous and challenging-to-implement controls, largely because of undocumented and overlooked scientific approaches.

In 2020, the European Court of Justice invalidated the EU-US data flows agreement known as Privacy Shield, citing concerns over the use and potential abuse of US intelligence activities (Data Privacy Manager, 2023). This ruling led to significant changes in the use of Standard Contractual Clauses (SCCs), making their use more stringent. However, despite these changes, Meta and many other US-based companies continued to rely on SCCs without implementing additional compensating controls. The imposed fine requires Meta Ireland to cease data transfers to the US and bring processing operations into compliance with Chapter 5 of the GDPR. This specific chapter of the GDPR focuses on ending the unlawful processing and storage of personal data of EU/EEA users in the US (Data Privacy Manager, 2023).

Controls are typically categorized as technical, administrative, and physical, and they can be implemented in various preventive, detective, and corrective measures. Meta's fine highlights failures in both administrative and technical controls. The administrative failure is attributed to non-compliance with the stricter use of SCCs. Implementing additional technical controls could have offered sufficient compensating measures and potentially reduced the fine resulting from the improper use of administrative controls. However, this scenario raises questions about the availability and effective utilization of privacy controls for adequate protection.

Several privacy frameworks support the implementation of individual controls. In October 2022, President Joe Biden recently signed an executive order titled 'Enhancing Safeguards for United States Signals Intelligence Activities' to address the EU's concerns about unrestricted US intelligence activities. This executive order is a step towards establishing an EU-US Data Privacy Framework that will define the requirements for data transfers between the two continents (European Data Protection Board, 2023). During the development of this framework, the National Institute of Standards and Technology (NIST) has produced a framework that can be used to map specific controls within it. Other notable frameworks include the Generally Accepted Privacy Principles, Organization for Economic Cooperation and Development Privacy Principles, and the Nymity Privacy Framework, among others. This paper will examine the relationship between choosing a privacy framework and implementing privacy controls.

NIST Privacy Framework

The NIST Privacy Framework, ratified in January 2020, emerged in response to the complex data landscape involving individuals and the associated risks. Organizations have grappled with cybersecurity for over two decades, and now they must also address privacy concerns. Often, organizations fail to grasp the potential consequences of privacy risks, which present a unique challenge distinct from cybersecurity-related risks. Couple this with the fact that cybersecurity and privacy risks are often hard to quantify and may be subjective (NIST, 2020).

Physical Controls

Physical controls provide protection against real-world physical attacks against the facility and devices (Chapple, Stewart, Gibson, 2021). Common physical controls include bollards, fences, security guards, and warning signs. As it pertains to privacy risk, leveraging privacy screen filters for laptops may reduce the risk of shoulder surfing. Shoulder surfing occurs when an individual is able to see data in an unauthorized manner on another individual's laptop. When organizations choose to use the NIST privacy framework, they must understand that proper control environment applies controls through physical, administrative, and technical. Therefore, reliance upon one category of control does not constitute adequate protection.

The crosswalk reflects physical controls throughout the framework. Beginning with the Protect function this seeks to develop and implement appropriate data processing safeguards as the outcome (NIST, 2020). Flowing down to the category of Identity Management, Authentication, and Access control organizations may find that the outcome for this category is: Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access (NIST, 2020). Drilling down to the subcategory PR.AC-P2, the outcome is the management of physical access to data and devices (NIST, 2020). The controls that fulfill this outcome include PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, and PE-9 (NIST, 2020). These controls are part of the physical and environmental protection family in NIST SP 800-53.

Corrective Controls. Corrective controls are a control that is used after an unwanted event has occurred (Gregory, 2019). Using the crosswalk to locate a physical control employing a corrective methodology can be found under PE-02. PE-02d is a control enhancement that specifies individuals are removed from the facility access list when access is no longer Required (NIST, 2022). This control meets the spirit of corrective as action is being taken to remove an individual who no longer is authorized to physically be in the facility.

Detective Controls. Detective controls are used to sense and detect problems as they occur (Gregg & Johnson, 2017). PE-03(02) is a control that seeks to determine if the organization performs security checks at the physical perimeter of the facility or system exfiltration of information or removal of system components (NIST, 2022).

Preventative Controls. A preventative control is deployed to thwart or stop unwanted or unauthorized activity from occurring (Chapple, Stewart, Gibson, 2021). PE-02(02) is a control in the NIST SP 800-53 that specifies two forms of identification are required for visitor access to the facility where the system resides (NIST, 2022). This is a preventative control as it seeks to verify the individual identity before allowing access to the facility.

Technical Controls

Technical Controls use some form of technology to address a physical security issue (Conklin & White, 2021). Notable examples of technical controls include firewalls, intrusion prevention and detection systems, and data loss prevention. Technical controls are present across various control families in NIST SP 800-53. It is common knowledge that log generation and retention is critical for piecing together the digital story when an issue arises. Therefore many of the controls listed for the selected outcome revolve around log generation.

Managing Data Privacy BY: Professor Jordan A. VanHoy

Taking a look at the control function of the framework, the category labeled data processing management aims to manage data consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (NIST, 2020). The subcategory outcome is CT.DM-P8 with a final outcome of audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization (NIST, 2020). Many controls in the NIST SP 800-53 help organizations satisfy this outcome. The listed controls for this particular set of outcomes include: AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, and AU-16.

Corrective Controls. AU-05 deals with the response to audit logging process failures. The spirit of the corrective control is to return to normal operations. AU-05a specifies that organizational personnel are alerted in the event of an audit logging process failure (NIST, 2022). AU-05b documents what actions are taken in the event of a audit logging process failure (NIST, 2022). Organizations will need to minimize the amount of missing logging and the control is centered around developing what actions are required to correct logging deficiencies.

Detective Controls. AU-03 is an excellent example of a detective control as it pertains to contents of audit records. Logs are of no value if the log is not verbose enough to explain what occurred. An individual logging into an administrative account is a significant event and should be recorded in the event it causes an incident. AU-03a directly matches this requirement by specifying audit records contain information that establishes what type of event occurred (NIST, 2022). This is detective in nature as when implemented correctly explains events such as administrator logon, failed logon attempt, privilege escalation, and account lockout.

Preventative Controls. AU-04(01) is a preventative control aimed at transferring audit logs to a different system, system component, or media other than the system or system component conducting the logging. This control holds unique value in the age of ransomware. If copies of backups and logging are kept at alternate locations it is possible to recover from ransomware and possess logs capable of explaining what occurred. This is preventing a single point of failure in the auditing and logging process.

Administrative Controls

Administrative controls are policies and procedures for managing security or privacy (Mehta, 2023). Examples of administrative controls include information security plans, acceptable use policies, security awareness training, and change management procedures. Best practices in the industry typically adopt a top-down approach, where organizational leadership takes the lead by actively engaging and demonstrating genuine concern. This approach often begins by establishing high-level policies that set the strategic direction for the organization before outlining the specific steps required to implement those policies. Whether it's authentication or the company travel policy, it's essential to define a strategic vision.

Examining the crosswalk, every portion of the framework will benefit from having administrative controls in place. Taking a look at the communicate function of the privacy framework, the objective is to develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks (NIST, 2020). The category is data processing awareness with the outcome of having individuals and organizations possessing reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organizations risk strategy to protect individuals' privacy (NIST, 2020).

Managing Data Privacy BY: Professor Jordan A. VanHoy

The subcategory is CM.AW-P3 with the granular outcome of system/product/service design enables data processing visibility (NIST, 2020). For these set of outcomes, PL-8 is a potential solution from the Planning family of controls found within the NIST SP 800-53.

Corrective Controls. PL-08(01)(a)[02] seeks to determine if the organization has a privacy architecture for the system that is designed using a defense in depth approach (NIST, 2022). By detailing policy requirements for concepts such as maximum tolerable downtime, mean time to recovery, and mean time to respond the organization sets the threshold for correcting issues after they have occurred. A defense in depth architecture allows for a multitude of controls to be implemented in support of the broader policy set by the organization. By possessing strategic direction on thresholds for taking action when an incident occurs, the organization can plan appropriately for supporting the objectives.

Detective Controls. Taken in another light, PL-08(01)(a)[02] can also incorporate administrative controls using detective methods. While the control is not explicitly detective in nature, defense in depth ensures that controls are in place and ready to assume risk should another control fail. An example of this is having policies that state the organization must have the ability to detect issues when they arise. Incorporation of a Security Information and Event Management tool would support log aggregation and the ability to detect issues as they arise.

Preventative Controls. PL-08a.02 describes a control in which an organization possesses a privacy architecture and describes the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals (NIST, 2022). This control is preventative in nature as having a well-defined and thought-out architecture backed by explicit requirements reduces the possibility for error or privacy gaps. Often times, organizations lack appropriate architecture diagrams making understanding of data traversal throughout a organization nearly impossible.

Conclusion

May 2023 brought significant GDPR enforcement concerns to Meta. Meta received a historic 1.2 billion euro fine and serves as a significant example of the growing importance of data protection and enforcement the regulations like GDPR and California Consumer Privacy Act (CCPA). This case study highlights the complex challenges organizations face in managing privacy controls effectively, especially when conducting business abroad. The management of privacy is more of an art than a science, characterized by ambiguous and challenging-to-implement controls, largely because of undocumented and overlooked scientific approaches.

The NIST Privacy Framework, established in 2020, provides a comprehensive structure for organizations to manage privacy risks. It comprises three key components: the core, profiles, and implementation tiers. The core defines activities and outcomes, while profiles serve as a roadmap for enhancing an organization's privacy posture. Implementation tiers offer a maturity model for understanding how the organization views privacy risk. Coupled with the NIST SP 800-53, various types of controls, including physical, technical, administrative, corrective, detective, and preventative controls, may be applied in protecting privacy and managing risks.

As environments continue to become more complex, it is essential to select the right controls and align them with their specific privacy needs and objectives. The NIST Privacy Framework offers specific sets of outcomes that organizations can center their privacy programs on. In this age where data privacy is a significant concern, organizations must continually assess and improve their control environments to protect individuals' privacy, ensure compliance, and build stakeholder trust.

Managing Data Privacy BY: Professor Jordan A. VanHoy

References

1. Chapple, M., Stewart, J. M., & Gibson, D. (2021). (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide. Sybex.
2. Conklin, W. A., & White, G. (2021). CompTIA Security+ All-in-One Exam Guide, Sixth Edition (Exam SY0-601). McGraw Hill Professional.
3. Data Privacy Manager. (2023). Meta Hit with Record €1.2B GDPR Fine. <https://dataprivacymanager.net/meta-hit-with-record-e1-2b-gdpr-fine/>
4. European Data Protection Board. (2023). EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en
5. Gregg, M., & Johnson, R. (2017). Certified Information Systems Auditor (CISA) CERT guide. Certification Guide.
6. Gregory, P. H. (2019). CISA Certified Information Systems Auditor All-in-One Exam Guide, Fourth Edition. McGraw Hill Professional.
7. Mehta, S. (2023). ISACA Certified in Risk and Information Systems Control (CRISC) Certification Guide: An Exam Guide for the Most Recent and Rigorous Risk and Audit Certification for Professionals. Packt Publishing.
8. National Institute of Standards and Technology. (2022). Assessing security and privacy controls in information systems and organizations. <https://doi.org/10.6028/nist.sp.800-53ar5>
9. National Institute of Standards and Technology. (2020). Privacy Framework. <https://www.nist.gov/privacy-framework/privacy-framework>



Welcome to the NOVEMBER 2023 issue of THE PACKET! I'm Professor Michael Galde, and it is my pleasure to present to you the latest insights and breakthroughs in the world of cybersecurity. In this month's edition, we delve into a series of compelling topics and expert analyses that are pivotal to understanding the current cyber landscape.

In this month's Hacks of the Month, Our section covers a spectrum of sophisticated cyber incidents:

- Iran's MuddyWater Group: An in-depth look at their latest espionage tactics.
- AvosLocker: How they're targeting essential US sectors amid a global uptick in cyber threats.
- Sandworm's Campaign: Unpacking their recent exploitation of Ukrainian telecom vulnerabilities.
- Microsoft's Expose: A formidable financial cyber threat comes to light.

In this month's Cyber News Updates, we provide a detailed analysis titled "The Evolving Threat Landscape of North Korean APTs." This piece is essential reading for anyone seeking to understand the complexities of state-sponsored cyber activities.

Exciting developments are afoot with the introduction of my small project "HexCheck: A Python Network Visualization Tool." This innovative tool promises to enhance your understanding of network dynamics through visual analysis and your ability to visualize if a system is up or down and running the services you require.

We're proud to feature an outstanding student research paper, "Covert Communications in Network Protocols: A Study of Techniques." This paper provides a nuanced exploration of the subtleties involved in hidden data transmission.

Our own Professor Jordan A. VanHoy offers his expertise in the compelling study "Managing Data Privacy," a timely piece given the ever-increasing importance of data security.

Finally, as we approach the end of the semester, I extend my best wishes to all students facing finals in the next few weeks. Your dedication and hard work have helped you get to where you are today. Let's keep the momentum strong and conclude this semester on a high note! Enjoy the insights, and may they inspire and inform your endeavors in the realm of cybersecurity.

CONTACT US

CIIO@EMAIL.ARIZONA.EDU

1140 N. Colombo Ave. | Sierra Vista, AZ 85635

Phone: 520-458-8278 ext 2155

<https://cyber-operations.azcast.arizona.edu/>

