Read more: Boosty

I. Introduction

Advanced persistent threat (APT) attacks spreading throughout the Asia-Pacific (APAC) region, attributed to a group known as Dark Pink, also referred to as the Saaiwc Group began as early as mid-2021, but escalated significantly in the latter part of 2022. Many of these attacks were directed at APAC countries, but the threat actors also expanded their scope to target a European governmental ministry.

In October 2022, Dark Pink initiated an unsuccessful attack against a European state development agency operating in Vietnam. The group employs a variety of tools and custom-built malicious software designed for data theft and espionage. A significant part of Dark Pink's success can be attributed to the spear-phishing emails used to gain initial access. These emails contain a shortened URL linking to a free-to-use file sharing site, where the victim is presented with the option to download an ISO image that contains all the files needed for the threat actors to infect the victim’s network.

Dark Pink APT attacks are characterized by their sophistication and versatility. The group uses spear-phishing emails as the initial access vector, luring victims into downloading a malicious ISO image. The group employs a suite of customized malware tools to execute their attacks. They also use advanced techniques to evade detection.

The consequences of a successful Dark Pink APT attack can be devastating for the affected organization and potentially for national security, given the high-profile nature of their targets. The group's advanced persistence mechanisms allow them to maintain access to a victim’s network for a long period of time, enabling them to continue to exfiltrate data and potentially cause further damage.

Timeline of Dark Pink APT Group's Operations

- **Mid-2021**: The Dark Pink APT group's activities are first observed.
- **2022**: Their operations escalate, particularly in the latter part of the year.
- **October 2022**: An unsuccessful attack is launched against a European state development agency operating in Vietnam.
- **January-April 2023**: New modules are uploaded to a GitHub account associated with the group, suggesting ongoing development of their toolset

II. Primary Objectives of Dark Pink APT Group

This part discusses the main goals of the Dark Pink APT, which include corporate espionage, document theft, and data exfiltration. It also mentions the group's links to a GitHub account where they store PowerShell scripts, ZIP archives, and custom malware. The primary objectives of the Dark Pink APT group include:

- **Corporate Espionage**: One of the main goals of the Dark Pink APT group is to conduct corporate espionage, which involves stealing sensitive information from corporations for competitive advantage or other malicious intent
- **Document Theft**: The group is actively engaged in the theft of documents, which likely contain confidential and proprietary information, from their targets
- **Audio Surveillance**: Dark Pink has the capability to capture audio through the microphones of compromised devices, which can be used for eavesdropping on private conversations and meetings
- **Data Exfiltration from Messaging Platforms**: The group also focuses on exfiltrating data from various messaging platforms, indicating an interest in personal communications and potentially sensitive information shared through these channels
- **Geographical Focus**: While the majority of Dark Pink's attacks have been directed at countries in the Asia-Pacific region, they have also targeted a European governmental ministry, showing an expansion in their geographical scope
- **Victim Profile**: Confirmed victims include military organizations in the Philippines and Malaysia, government agencies in Cambodia, Indonesia, and Bosnia and Herzegovina, as well as a religious organization, demonstrating the group's interest in high-value and diverse targets
- **Spear-Phishing for Initial Access**: A significant factor in the success of Dark Pink's operations is the use of spear-phishing emails that contain a shortened URL. This URL leads victims to a file-sharing site where they are tricked into downloading an ISO image containing malicious files necessary for network infection
- **Evolution of Exfiltration Techniques**: Dark Pink has evolved its data exfiltration techniques, moving from using email and public cloud services like Dropbox to employing the HTTP protocol and a Webhook service in more recent attacks

III. Tools Used by Dark Pink APT Group

This section introduces the tools widely used by Dark Pink APT Group to attack, gain access and exfiltrate data from devices across the world.

A. *Tools Used by Dark Pink APT Group*

The Dark Pink APT group utilizes a suite of customized malware tools in their attacks, primarily relying on spear-phishing emails to gain access to their targets' networks. Notably, they use TelePowerBot and KamiKakaBot, which are designed to exfiltrate sensitive data from compromised hosts. They have been linked to a new version of the KamiKakaBot malware, which is delivered via phishing emails containing a malicious ISO file. This file contains a WinWord.exe file, which is used to stage a dynamic link library (DLL) sideloading attack. The group has also been found to use legitimate MsBuild.exe to run the KamiKakaBot malware on victims' devices. The malware's obfuscation technique has improved to better evade anti-malware measures, and it uses an open-source .NET obfuscation engine to hide itself. The group also uses a special messenger exfiltration utility named ZMsg, which is downloaded from GitHub and used to steal communications from Viber, Telegram, and Zalo.

In addition to these, Dark Pink has been found to use DLL side-loading and event-triggered execution methods to run its payloads. They also employ a variety of techniques and services for data exfiltration, including email, public cloud services like Dropbox.

B. *Modifications Made to the Tools Used by Dark Pink APT Group*

The group has links to a GitHub account where they store PowerShell scripts, ZIP archives, and custom malware designed for future deployment on targeted devices. They have also been observed exploiting the WinRAR 0-Day vulnerability (CVE-2023-38831) in their attacks to execute malicious unauthorized code. They have been exploiting this vulnerability by embedding malicious executables within commonly used file types, such as PDFs and JPGs, within ZIP archives. This tactic allows attackers to install malware on a user's device without arousing suspicion, as the victim believes they are interacting with a harmless file. The exploitation file constructed by Dark Pink includes a PDF bait file and a folder with the same name. Inside the folder, there are two files: one is an exe program with the same name as the PDF bait file, and the other is a library file named ‘twinapi.dll’. The group also uses techniques such as USB infection and DLL exploitation.

C. *New Tactics Employed by Dark Pink APT Group*

New tactics employed by the Dark Pink APT group include the use of different Living Off the Land Binaries (LOLBins) techniques and leveraging the functionalities of an MS Excel add-in to ensure persistence. They have also been found to exfiltrate stolen data over HTTP using services like webhook.site, which allows them to set up temporary endpoints to capture and view incoming HTTP requests. Payloads are also being distributed through the TextBin.net service, and the group has been observed exfiltrating stolen data over HTTP using a service. These new tactics indicate the group's ongoing efforts to enhance their capabilities, evade detection, and maintain control over compromised networks.

IV. Data Extraction Techniques

The data extraction techniques include:

- **Variety of Exfiltration Techniques**: Dark Pink has employed a range of techniques and services to exfiltrate data from their targets. This demonstrates the group's adaptability and sophistication in ensuring successful data theft
- **Public Services**: Publicly available cloud services such as Dropbox have been used by Dark Pink for data exfiltration
- **Use of Email and Cloud Services**: In previous attacks, the group sent stolen information via email or utilized public cloud services like Dropbox for data exfiltration. This indicates that they leveraged commonly used communication and storage platforms to move data out of compromised networks
- **Shift to HTTP Protocol and Webhook Service**: More recently, Dark Pink has shifted to using the HTTP protocol and a Webhook service to exfiltrate stolen data. This change in tactics could be an attempt to evade detection by security systems that are more focused on traditional exfiltration methods
- **Evolution of Tactics**: The evolution from using email and cloud services to HTTP and Webhook services suggests that Dark Pink is continuously refining its exfiltration methods to stay ahead of cybersecurity defenses

As mentioned above The Dark Pink APT group uses Telegram and a service called Webhook for data exfiltration.

Telegram: Dark Pink uses Telegram for both command-and-control and data exfiltration. The group has been observed to use a Telegram bot for executing commands and managing data theft. The stolen data is often sent to a Telegram chat in a zip archive. This method provides a secure and encrypted channel for data exfiltration, making it harder for security systems to detect and block the data transfer

Webhook: Dark Pink has also been observed to use a service called Webhook.site for data exfiltration. Webhook.site is a service that allows users to create temporary endpoints to capture and view incoming HTTP requests. Dark Pink uses this service to exfiltrate stolen data over HTTP. This method allows the group to send data to a specific URL, which can then be accessed and retrieved by the threat actors. This technique can be used to evade detection by security systems that are more focused on traditional exfiltration methods

The group uses a private GitHub repository to host additional modules downloaded by its malware. They have also developed new data exfiltration tools to dodge detection. One of the group's techniques involves the use of the KamiKakaBot malware, which is primarily designed to steal data stored in web browsers such as Chrome, Edge, and Firefox, including saved credentials, browsing history, and cookies. Dark Pink has also been found to exfiltrate stolen data over HTTP using a service.

Furthermore, they employ a specialized toolkit that includes a custom information stealer coded in .NET, known as Cucky. This tool is proficient in extracting passwords, browsing history, login credentials, and cookies from a range of web browsers targeted by the group. The stolen data is stored locally in the %TEMP%\backuplog directory, without transmitting it over the network

V. Dark Pink Origins and Affiliates

Many Dark Pink's attacks were directed at countries in the Asia-Pacific region, although the group expanded its scope to target a European governmental ministry. This indicates a broadening of their operational scope.

A. Industries Targeted by Dark Pink APT Group

The Dark Pink APT group has targeted a wide range of industries, including government, military, non-profit organizations, educational institutions, and development agencies across the Asia-Pacific region and Europe. Specific industries mentioned in the context of their attacks include retail, healthcare, gaming, technology, software, pharmaceuticals, aerospace, defense, automotive, and media.

B. New Industries Targeted by Dark Pink APT Group

The Dark Pink APT group has expanded its target industries and geographical reach. While the group was previously thought to focus mainly on Southeast Asian countries, new victims have been identified in Belgium, Thailand, and Brunei. The group has been linked to five new attacks aimed at various entities in these countries, including educational institutions, government agencies, military bodies, and non-profit organizations. This indicates the group's continued focus on high-value targets and its expansion into new industries and regions.

In addition to these, the group has also targeted entities in the retail, healthcare, gaming, technology, software, pharmaceuticals, aerospace, defense, automotive, and media industries. The group's targets include diplomatic, military, and various industries in countries such as Cambodia, Indonesia, Malaysia, the Philippines, Vietnam, Bosnia and Herzegovina, and others

VI. Initial Access and Trojan Execution and Persistence

This section explains how Dark Pink gains initial access to their targets, primarily through spear-phishing emails containing a shortened URL that leads to a free-to-use file sharing site.

The initial methods include:

- **Spear-Phishing Emails**: A significant part of Dark Pink's success can be attributed to the spear-phishing emails used to gain initial access. These emails contain a shortened URL linking to a free-to-use file sharing site
- **ISO Image**: The victims are presented with the option to download an ISO image from the file sharing site. This image contains all the files needed for the threat actors to infect the victim's network
- **Trojan Execution and Persistence**: Once the ISO image is downloaded and opened, it triggers the execution of a Trojan on the victim's device. This Trojan is designed to maintain persistence on the infected system, allowing the threat actors to maintain access over an extended period

Spear-phishing is a type of phishing attack that targets specific individuals or groups within an organization. It is a potent variant of phishing, a malicious tactic which uses emails, social media, instant messaging, and other platforms to get users to divulge personal information or perform actions that cause data loss or financial loss. Spear-phishing attacks are highly personalized and often involve prior research about the target. The attackers disguise themselves as a trustworthy friend or entity to acquire sensitive information, typically through email or other online messaging. The goal of spear-phishing is to steal sensitive information such as login credentials or infect the victim's device with malware. Spear-phishing is a targeted form of phishing where cybercriminals send highly convincing emails to specific individuals within an organization. These emails often contain malicious attachments or links that, when clicked, can deliver Trojans to the victim's system. For instance, the Ursnif Trojan uses a company's stored emails to send what appear to be legitimate emails. These emails contain a Word document attachment with a malicious macro that downloads the malware. Once the payload is executed, the victim's computer becomes a delivery vehicle to spread within an organization

ISO images are files that contain a complete copy of a CD, DVD, or other types of media. They are often used to distribute software or data. Cybercriminals have started using ISO files for their initial compromise because they can help evade security checks designed to look for zipped files. Malicious ISO files have been used to deliver various types of malware, including the IcedID, LokiBot, and NanoCore trojans. The ISO file is typically delivered as part of a malspam campaign, and when the user clicks on the ISO file, it creates a new virtual hard drive disk. ISO images can also be used to deliver malware. Cybercriminals have been observed using ISO image files in malicious spam campaigns to deliver Trojans like LokiBot and NanoCore. The ISO file is delivered as a ZIP archive via a malicious spam mail campaign. When the user clicks on the ISO file, it creates a new virtual hard drive disk. The ISO file contains a malicious LNK file and a hidden directory containing a payload. When the victim clicks on the LNK file, it triggers the execution of the payload. This technique has grown in use as threat actors look to evade Mark-of-the-Web controls. ISO files are often overlooked by antivirus software, making it more likely that attackers can deliver their payload undetected.

Trojan execution refers to the process of a Trojan horse program being run on a computer system. Trojans are malicious programs that disguise themselves as legitimate software. They can be used to gain unauthorized access to a computer system and perform various malicious activities. For example, the IcedID malware contained within an ISO image is executed when the user clicks on a LNK file within the virtual hard drive created by the ISO file. Trojans use various persistence techniques to ensure they continue to run on a system, even after it has been rebooted or after the security software has been run. Some common methods include modifying the registry, creating scheduled tasks, installing itself as a service, or using rootkits to hide its presence. Other techniques include abusing legitimate operating system processes, such as adding an entry to the run keys in the Windows Registry or the Startup folder, which ensures that any referenced programs will be executed when a user logs in. Some less common but more sophisticated methods include abusing Image File Execution Options for debugging and hijacking the shortcut icons Target attribute.

Persistence refers to the techniques used by attackers to maintain access to a compromised system even after the system has been rebooted or the initial infection vector has been removed. Attackers use various methods to achieve persistence, including adding entries to the run keys in the Windows Registry or the Startup folder, so that their malicious programs are executed every time the system is started or a user logs in. Persistence allows attackers to maintain access to a network as

OVERKILL SECURITY

they search for the data they want, and it can also be used to spread other malware. Some Trojans, like the Ursnif Trojan, use fileless persistence techniques, which involve storing an encoded command inside a registry key and launching it using the Windows Management Instrumentation Command-line (WMIC).

A. Examples of Trojans Delivered Through Spear-Phishing Attacks

Trojans can be delivered through spear-phishing attacks, which are highly targeted and often involve sophisticated social engineering techniques:

- **OutSteel and SaintBot**: These Trojans were used in attacks targeting an energy organization in Ukraine as part of a larger campaign
- **Ursnif**: This banking Trojan uses a company's stored emails to send what appear to be legitimate emails with a Word document attachment containing a malicious macro that downloads the malware
- **TrickBot**: An advanced Trojan that has been spread primarily by spear-phishing campaigns using tailored emails with malicious attachments or links
- **IcedID**: Delivered within an ISO image as part of a malspam campaign, this Trojan has been used to evade Mark-of-the-Web controls.

B. Common Signs of Trojan Infection Using ISO Images

When a computer has been infected with a Trojan that uses ISO images to deliver malware, there may be several signs indicating the infection:

- **Unexpected Advertisements**: Advertisements may appear in places they shouldn't be, which can be a symptom of adware, a type of Trojan
- **Changed Homepage**: The web browser's homepage might change without permission, indicating that a browser hijacker, another type of Trojan, may be present
- **Suspicious Processes**: Processes related to the Trojan, such as "Your File Is Ready To Download.iso," may run in the background without the user's knowledge
- **Redirected Links**: Website links may redirect to sites different from what was expected, which can be a sign of a Trojan manipulating web traffic
- **Corrupted Files**: Opening a file and finding it corrupted could be a red flag that ransomware or another form of malware has infected the system
- **Strange Popups**: Some forms of malware can disguise themselves as legitimate programs, and unexpected popups may be a sign of such deceptive tactics
- **New or Modified Files**: Some types of malware may make copies of files or introduce new files into the system, often with generic-sounding names to avoid detection

VII. Indicators of Compromise (IOCs)

The Indicators of Compromise (IOCs) related to the Dark Pink APT group, as listed in the CyberInt research, include:

IP Addresses:

- 185.141.63[.]128
- 185.141.63[.]129
- 185.141.63[.]130
- 185.141.63[.]131

Domains:

- hxxp://185.141.63[.]128/office/update/
- hxxp://185.141.63[.]129/office/update/
- hxxp://185.141.63[.]130/office/update/
- hxxp://185.141.63[.]131/office/update/
- hxxp://185.141.63[.]128/office365/update/
- hxxp://185.141.63[.]129/office365/update/
- hxxp://185.141.63[.]130/office365/update/
- hxxp://185.141.63[.]131/office365/update/

File Hashes:

- 5f4dcc3b5aa765d61d8327deb882cf99
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6
- 098f6bcd4621d373cade4e832627b4f6

OVERSILL SECURITY