Cyber Threat Advisory

JULY 2023

Contents

Monthly Highlights - July

1. **Apple patches exploits used in spy campaign 'Operation Triangulation'**

   Apple has released updates for the iOS remote code execution (RCE) flaws that have already been used in the field as part of the cyberespionage effort known as Operation Triangulation. The campaign took advantage of two zero-click iMessage exploit and compromises that didn't require any user input and were predicated on two weaknesses in the kernel and Webkit, respectively. Just two weeks after the Russian cybersecurity company disclosed finding an advanced persistent threat (APT) actor releasing zero-click iMessage attacks on Russian iOS devices, Apple has credited Kaspersky Lab with finding these vulnerabilities.

   The exploited flaws, according to Apple, include difficulties with memory corruption in the kernel (CVE-2023-32434), which allows software to run arbitrary code with kernel privileges, and a fault with WebKit (CVE-2023-32435), which permits code execution through web content. Thankfully, Apple has released patches for these problems in the most recent versions of its operating systems, iOS 16.5.1, iPadOS 16.5.1, iOS 15.7.7, and iPadOS 15.7.7. Both the most recent version (iOS 16.5.1) and the first vulnerable version (prior to iOS 15.7) have received the updates. Apple stated that the attacks have only been detected on iOS 15.7 and earlier-running devices. Patches for macOS and watchOS were also issued in addition to updates for iPhones and iPads.

2. **Ransomware attacks pose communications dilemmas for local governments**

   The City of Dallas, Texas, was targeted by a ransomware assault in the early hours of May 3, for which the Royal ransomware group subsequently claimed responsibility. The event severely impacted the city's police, fire rescue, water service payment, and development systems, among others, causing several agencies to switch to handwritten and radio-related communications. The city stated that more than 90% of the work to repair the systems was finished in a report dated May 31 that was made public on June 9. Departments that switched back to manual labour,

nevertheless, continued to update the data in their systems. The city has kept the public in the dark about the attack and continues clean-up, stating that "This is an ongoing criminal investigation." The city is unable to remark on specifics since doing so may impede the inquiry or reveal loopholes that an attacker could exploit.

The mayor and city council were instructed not to disclose any information on how the city responded to the assault in an email sent on June 1 by Catherine Cuellar, Dallas' director of communications, outreach, and marketing. She suggested that they limit the remarks made by their constituents to three. "We appreciate your inquiry. Rest assured that we are collaborating with other experts and law enforcement, and that our investigation is ongoing. We will provide updates as needed."

Cuellar answered via email to CSO's request for further details about the assault on June 14 by stating that "The City of Dallas remains dedicated to openness and keeping our community aware with important developments regarding the ransomware incident. We take our obligation to provide the public with accurate information very seriously. This situation is still being investigated into at this time. As additional information becomes available, we will continue to provide updates as appropriate on DallasCityNews.net."

Dallas' reluctance to divulge information about the event emphasises the fine line that local governments must tread when informing taxpayers about the specifics of ransomware attacks, according to cybersecurity experts. On the one hand, affected individuals need to be aware of the essential details regarding the services that have been disrupted by ransomware incidents. On the other side, providing excessive information could aid an attacker and possibly divulge sensitive data, giving the threat actors more confidence or leaving the government up to greater liabilities.

3. **Romanian cybercrime gang Diicot builds DDoS botnet with Mirai variant**

According to the researchers, a cybercriminal group called itself Diicot is involved in massive SSH vulnerability scanning and deployment of variant Mirai IoT botnets on vulnerable devices. Additionally, for servers with more than four CPUs, the group is deploying a cryptocurrency mining payload. "Although Diicot have traditionally been associated with cryptojacking campaigns, Some evidences were discovered by Cado Labs for the group deploying an off-the-shelf Mirai-based botnet agent, named Cayosin," researchers from Cado Security said. "Deployment of this agent was targeted at routers running the Linux-based embedded devices operating system OpenWrt."

4. **Trend Micro adds generative AI to Vision One for enhanced XDR**

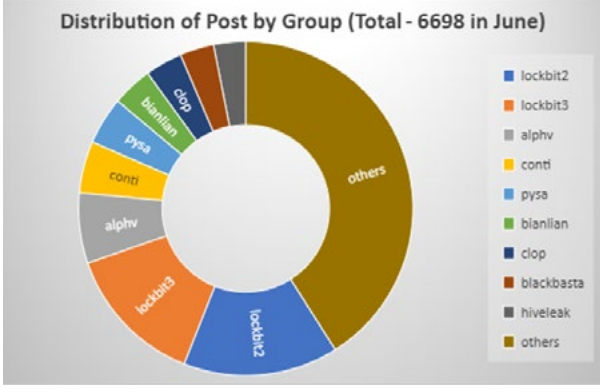
With a new AI tool called Companion, Trend Micro has announced that it will integrate generative artificial intelligence into its flagship Vision One platform. Companion uses advanced AI/machine learning analytics and correlated detection models to enhance extended detection and response (XDR) capabilities, according to the cybersecurity vendor. In a press release, Trend Micro claimed that it had been designed to enhance security operations, improve accessibility and effectiveness as well as speed the search for threats by analysts of different skill levels. It adds that this release is the first stage of a multi quarter rolling out of Artificial Intelligence and wide language Model LLM capabilities, which are incorporated into Vision One. The popular trend in cybersecurity right now is the introduction of AI technologies, such as Generative Automatic Intelligence and LLM enhanced security threat detection and response, which are being implemented by various service providers to enhance their products' smartness, speed, conciseness.

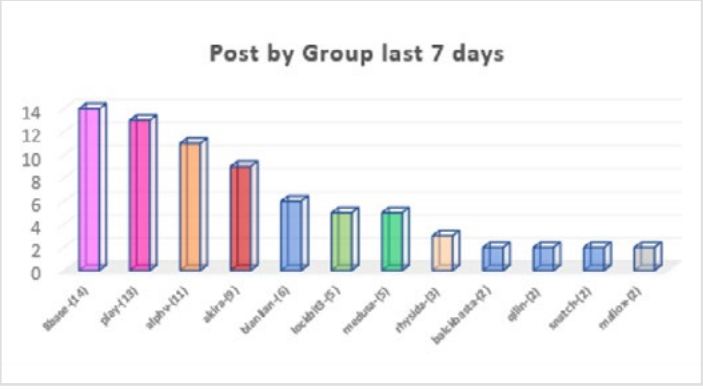
5. **Millions of GitHub repositories vulnerable to RepoJacking: Report**

In AquaSec's analysis of 1% of the GitHub repositories, it turned out that around 37,000 were vulnerable to RepoJacking, which included websites like Google and Lyft. According to research from AquaSec, more than a million GitHub repositories could be at risk of RepoJacking, which enables attackers to perform code execution on the internal and external environments of companies or their customers. Organizations' usernames and repository names are listed in the GitHub database. An organization can change GitHub usernames or repository names if there is a change of manager, new brand name etc. In order to prevent the breaking of dependencies between projects that use code from repositories who change their names, a redirect has been set up. This redirection is not valid when an old name is registered by someone else.

RepoJacking is an attack in which an attacker registers a username and creates a repository that has been used by an organization in the past but has changed its name. This means that any project or code that relies on the dependencies of the attacked project to fetch the dependencies and code from the attacker-controlled repository that could contain malware. According to AquaSec, "To avoid attackers gaining access to an earlier repository name, GitHub has a few restrictions. However, these restrictions are only applied to popular repositories that were popular prior to the renaming, and recent research has shown that many of them have been circumvented, allowing attackers to open any repository they desire."

Ransomware Engagement Tracker



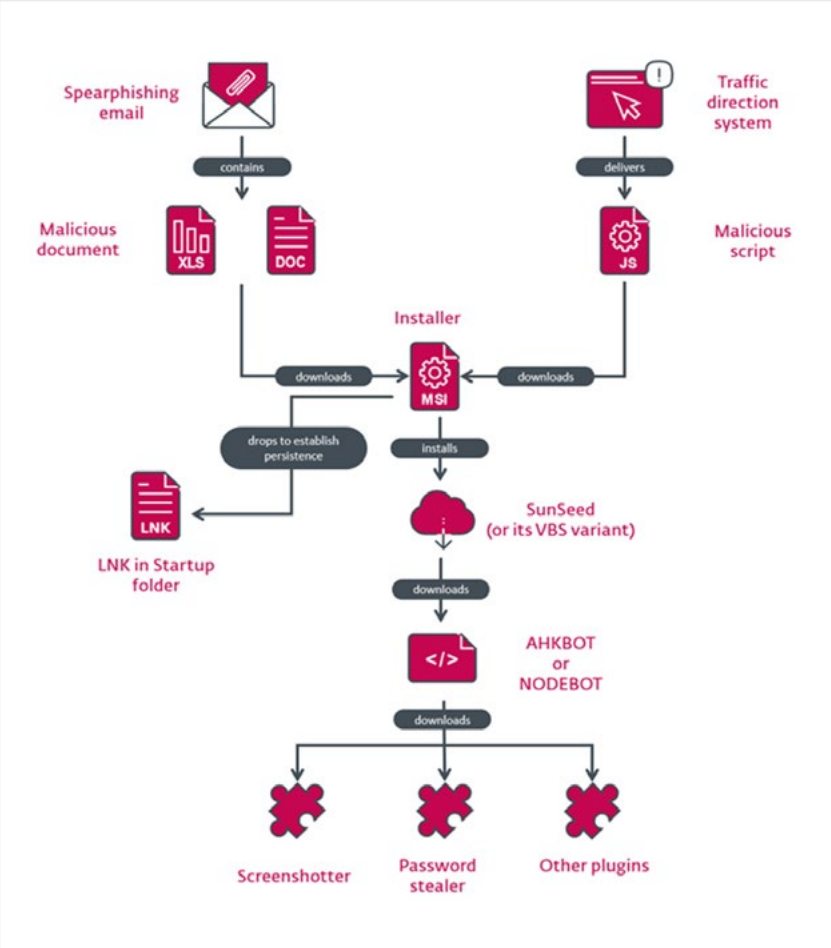


Asylum Ambuscade hackers mix cybercrime with espionage

- Cyber espionage and cybercrime were recently reported in attacks on small to medium-sized businesses around the world by a hacking gang known as Asylum Ambuscade.
- In an analysis released on Thursday, ESET stated that the crimeware organization "targets bank customers and cryptocurrency traders in various regions, including North America and Europe. Asylum Ambuscade also conducts espionage against governments in Central Asia and Europe."
- Asylum Ambuscade was originally identified by Proofpoint in March 2022 as a nation-state-sponsored phishing campaign that sought to gather information on the flow of refugees and supplies in the region by targeting European governmental organizations.
- The attacker wants to steal sensitive data and login details for web email accounts from official government email portals.

Detection:

- The attacks begin with a malicious Excel spreadsheet attachment that, when opened, either uses VBA code or the Follina vulnerability (CVE-2022-30190) to download an MSI package from a remote site.
- The installer, on the other hand, launches a downloader called SunSeed (or a Visual Basic Script equivalent) that, in turn, downloads the malicious software known as AHK Bot, which is based on AutoHotkey, from a remote server.
- Asylum Ambuscade is renowned for its worldwide cybercrime rampage that has claimed over 4,500 victims since January 2022, with the bulk of them being in North America, Asia, Africa, Europe, and South America.
- According to ESET researcher Matthieu Faou, "The targeting is very broad and mostly includes individuals, cryptocurrency traders, and small and medium-sized businesses (SMBs) in various verticals."
- The targeting of SMBs is probably an attempt to monetize the access by selling it to other cybercriminal groups for illegal gains, even though one part of the attacks is aimed to steal cryptocurrency.
- Except for the initial intrusion vector, which involves the use of a malicious Google Ad or a traffic direction system (TDS) to drive potential victims to a fake website that distributes a JavaScript file infected with malware, the compromise chain follows a similar pattern.
- The assaults have also made use of a Node.js version of AHK Bot with the codename NODEBOT, which is then used to download plugins for collecting screenshots, stealing passwords, and other malicious functions.



Prevention

- Block unknown scripts to run.
- Patch all DLL & javascript files in production.
- Do not click on the malicious link.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connection.
- Do not install unwanted application from untrusted source.
- Do not use malicious/free VPN to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

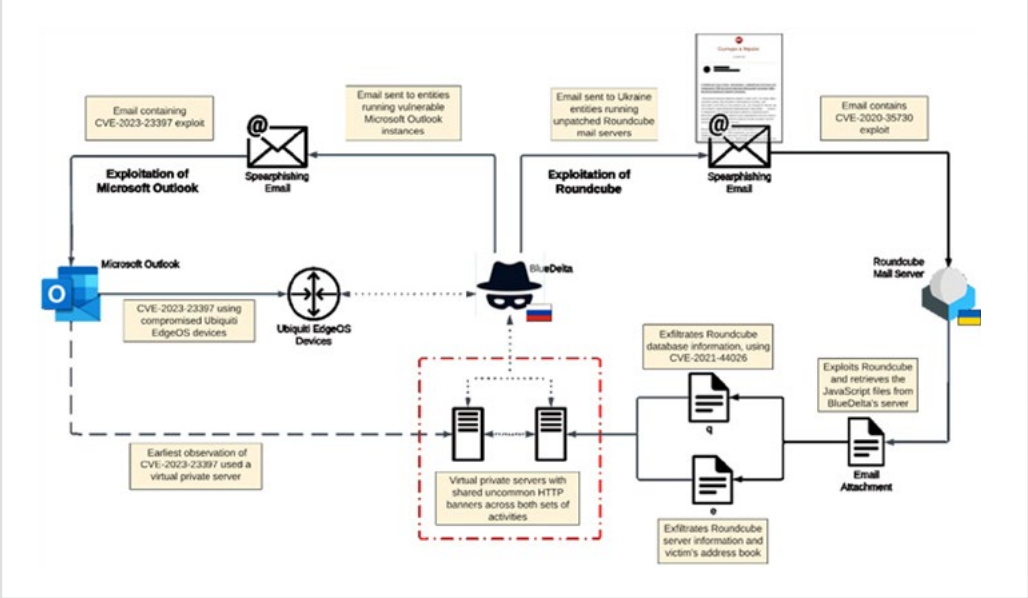
Remediation

- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving of data through communication channels.
- Update your machine & servers on monthly basis.
- Enable packet filtration through firewall.
- Configured DLP in environment in a proper way.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

Microsoft warns of widescale credential stealing attacks by Russian hackers

- Microsoft has revealed that it has noticed an increase in credential-stealing activities carried out by the Midnight Blizzard hacking collective, which is linked to the Russian government.
- Governments, IT service providers, NGOs, defence, and important manufacturing sectors are the targets of the incursions, which used residential proxy services to conceal their original IP address, according to the threat intelligence team of the tech giant.
- Other tracking names for Midnight Blizzard, once known as Nobelium, include APT29, Cosy Bear, Iron Hemlock, and The Dukes.
- The organization, which gained notoriety after compromising the SolarWinds supply chain in December 2020, has persisted in using covert technology in its targeted assaults on foreign ministries and diplomatic organizations.

Detection



- Microsoft stated in a series of tweets that "credential attacks use a variety of password spray, brute-force, and token theft techniques." The actor "conducted session replay attacks to gain initial access to cloud resources by leveraging stolen sessions likely acquired via illicit sale," Microsoft added.
- The IT giant also criticised APT29 for trying to disguise connections made with stolen credentials by employing residential proxy services to send malicious traffic.
- The news comes as Recorded Future revealed a fresh spear-phishing attack launched in November 2021 against Ukrainian military and government institutions by APT28 (also known as BlueDelta, Forest Blizzard, FROZENLAKE, Iron Twilight, and Fancy Bear).
- To conduct reconnaissance and acquire information, the attacks made use of emails with attachments that exploited numerous vulnerabilities in the free and open-source Round cube webmail software (CVE-2020-12641, CVE-2020-35730, and CVE-2021-44026).
- Following a successful intrusion, Russian military intelligence hackers were able to install malicious JavaScript scripts that stole contact lists from the targeted individuals and forwarded their incoming emails to an address under their control.
- "The campaign displayed a high level of preparedness, quickly weaponizing news content into lures to exploit recipients," the cybersecurity firm stated. The subject lines and substance of the spear-phishing emails mirrored those of reliable media sources and covered news topics pertaining to Ukraine.
- "BlueDelta will almost certainly continue to prioritize targeting Ukrainian government and private sector organizations to support wider Russian military efforts," Recorded Future concluded.

Prevention

- Block unknown scripts to run.
- Do not click on the malicious link.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connection.
- Do not install unwanted application from untrusted source.
- Do not use malicious/free VPN to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable SSL with SMTP protocol for safe transmission.
- Enable limitations on administrative access or rights.

Remediation

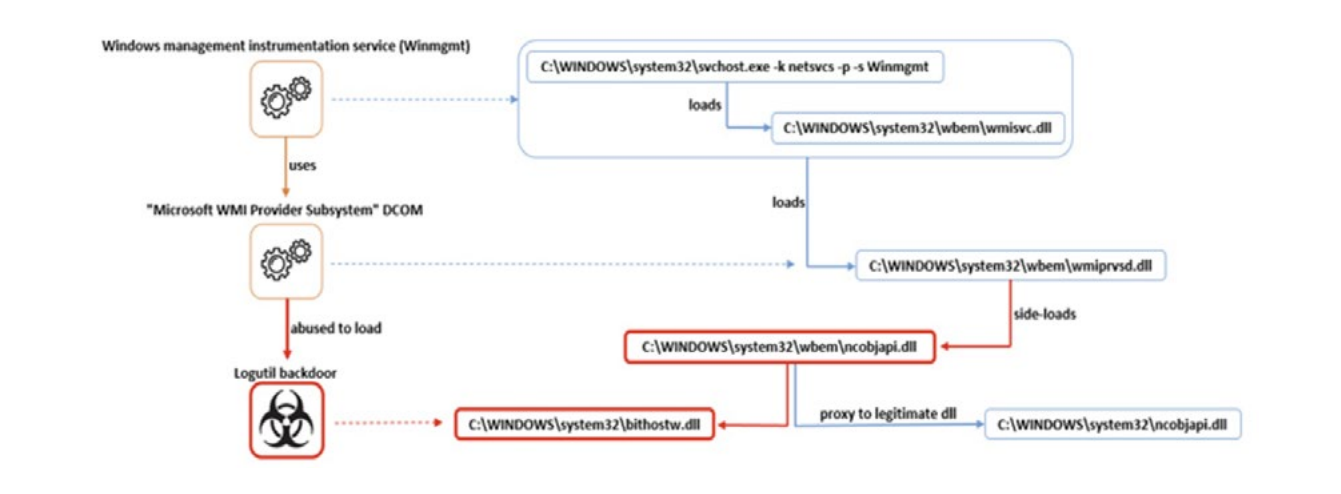
- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving of data through communication channel.
- Update your machine & servers on monthly basis.
- Enable packet filtration through firewall.
- Configured DLP in environment in a proper way.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

Experts uncover year-long cyber attack on IT firm utilizing custom malware RDStealer

- A unique piece of malware named RDStealer was used in a highly targeted cyber attack against an East Asian IT firm.
- The operation had the aim of compromising passwords and data exfiltration, according to a technical report provided to The Hacker News by Bitdefender security expert Victor Vrabie.
- Evidence acquired by the Romanian cybersecurity company reveals that the RedClouds campaign began in the first half of 2022. The targeting fits with the motives of threat actors located in China.
- Before switching to custom malware in late 2021 or early 2022 to avoid discovery, the operation relied on widely accessible remote access and post-exploitation tools like AsyncRAT and Cobalt Strike in its early stages.

Detection

- The use of Microsoft Windows directories like System32 and Programme Files to store the backdoor payloads, which are probably not scanned by security tools, is a common evasion technique.
- "C:Program FilesDellCommandUpdate," which is the directory for a genuine Dell application called Dell Command | Update, is one of the subfolders in question.
- The threat actor established command-and-control (C2) domains like "dell-a[.]ntp-update[.]com" to blend in with the target environment, which supports this line of thinking.
- The intrusion set is distinguished by the utilisation of a server-side backdoor known as RDStealer, which focuses on continuously collecting host-generated clipboard material and keyboard data. At this time, it is unknown how the RDP servers came to be compromised.



- But what distinguishes it from other malware is its ability to "monitor incoming RDP [Remote Desktop Protocol] connections and compromise a remote machine if client drive mapping is enabled."
- Thus, when a new RDP client connection is discovered, RDStealer issues commands to exfiltrate sensitive data from programmes like mRemoteNG, KeePass, and Google Chrome, including browsing history, credentials, and private keys.
- Additionally, additional Golang-based proprietary malware called Logutil is installed on the connecting RDP clients to retain a persistent foothold on the target network utilising DLL side-loading techniques and simplify command execution.

Prevention

- Block unknown scripts to run.
- Do not click on the malicious link.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the RDP feature for unknown connection.
- Do not install unwanted application from untrusted source.
- Do not use malicious/free VPN to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable limitations on administrative access or rights.

Remediation

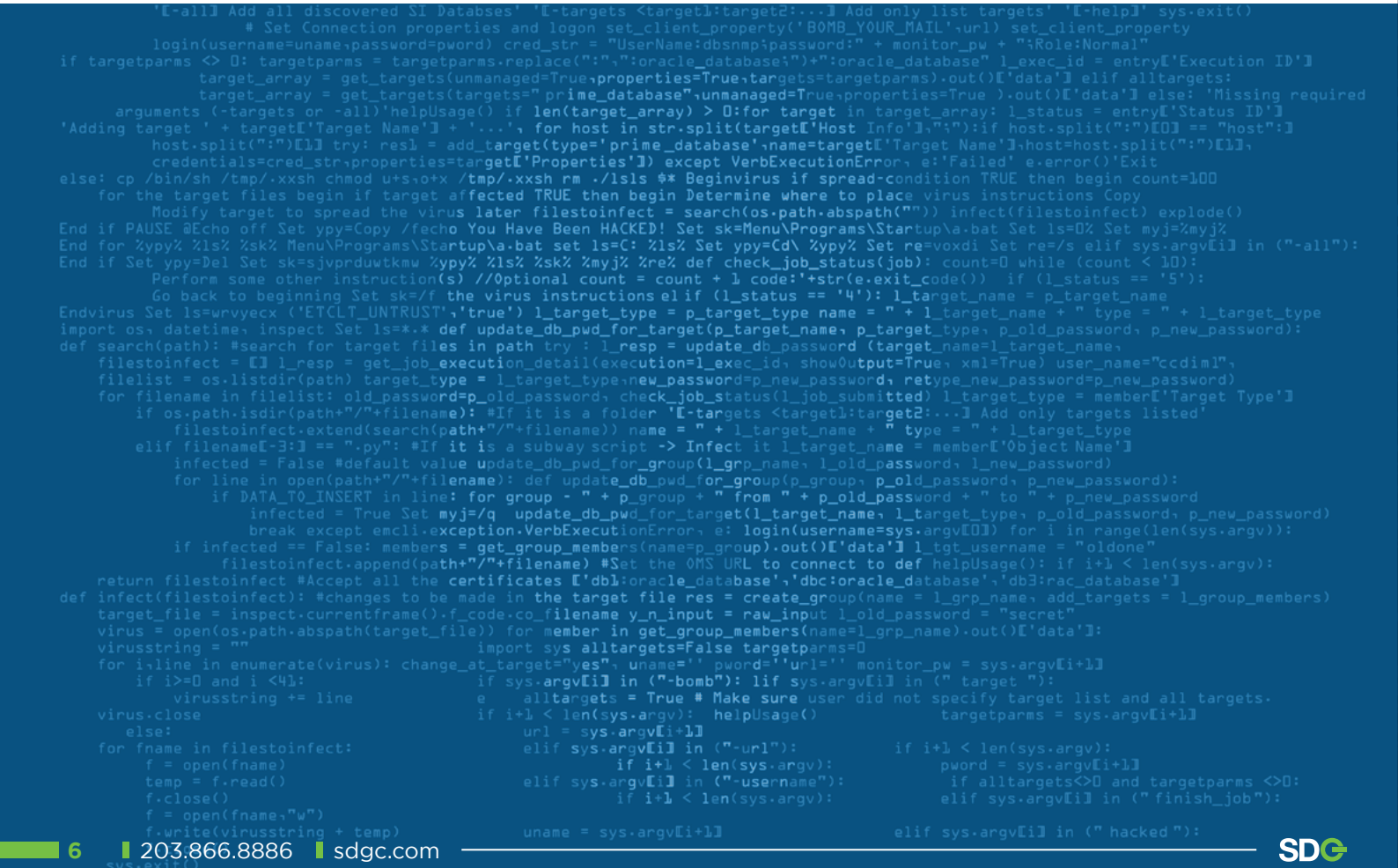
- Monitor event logs.
- Administrators should limit port proxy usage within environments.
- Download only trusted software from known sites.
- Use post method for sending & retrieving of data through communication channel.
- Update your machine & servers on monthly basis.
- Enable packet filtration through firewall.
- Configured DLP in environment in a proper way.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network.
- Use trusted anti-malware & anti-phishing programs.
- Enable two-factor authentication for transferring data packets.

Dark Pink APT group leverages TelePowerBot and KamiKakaBot in sophisticated attacks

- Five new attacks against distinct targets in Belgium, Brunei, Indonesia, Thailand, and Vietnam have been connected to the threat actor known as Dark Pink.
- This indicates the hostile crew's persistent focus on high-value targets and includes educational institutions, governmental organizations, military organizations, and non-profit organizations.
- Advanced persistent threat (APT) actor Dark Pink, also known as Saaiwc Group, is thought to have originated in the Asia-Pacific region. Its assaults typically target East Asian and, to a lesser extent, European targets.
- The organization uses a collection of unique malware tools, like TelePowerBot and KamiKakaBot, that perform a variety of tasks to extract sensitive data from infected machines.

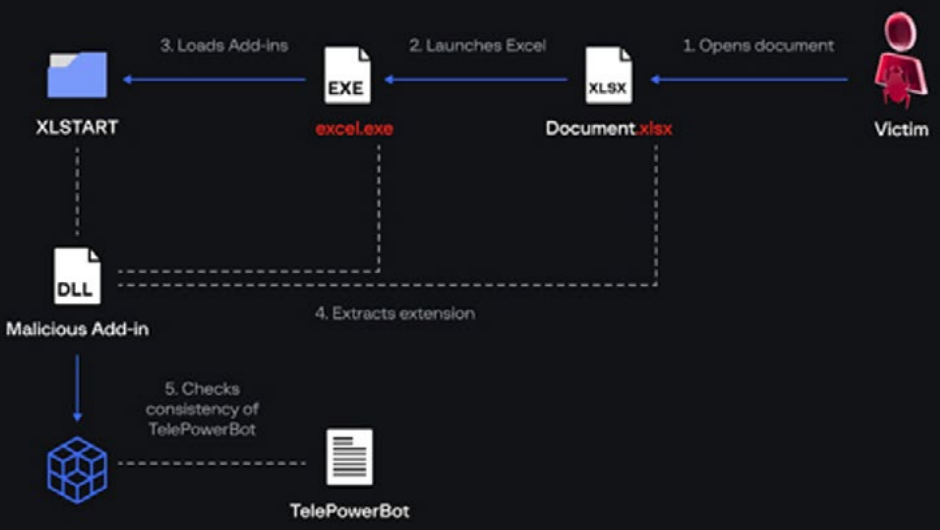
Detection

- The gang deploys numerous death chains using sophisticated proprietary tools and spear-phishing emails.
- Once within a target's network, attackers deploy sophisticated persistence measures to avoid detection and keep control of the compromised system.
- The findings also point out certain significant changes made to the Dark Pink assault sequence to thwart investigation and allow for upgrades to KamiKakaBot, a Telegram bot that executes commands from a threat actor-controlled Telegram channel.
- Notably, the most recent version divides its functionality into two separate parts: one for managing devices and the other for gathering useful data.
- Additionally, a fresh GitHub account linked to the threat actor was discovered, which is where PowerShell scripts, ZIP packages, and unique malware are hosted for later installation on victims' computers. The uploads of these modules took place between January 9 and April 11, 2023.
- Along with employing Telegram for command and control, Dark Pink has also been seen using the webhook[.]site service to leak stolen data over HTTP. Another noteworthy feature is the usage of a Microsoft Excel add-in to guarantee TelePowerBot's persistence inside the infected host.
- "With webhook[.]site, it is possible to set up temporary endpoints in order to capture and view incoming HTTP requests," said Polovinkin. The threat actor set up transient endpoints and delivered victims' sensitive data.
- Despite its espionage intentions, Dark Pink is still a mystery. However, it's possible that the hacker team's victimology footprint is larger than previously thought.



GROUP-IB

Consistency check of the TelePowerBot launch



Source: Group-IB, 2023.

Prevention

- Block unknown scripts to run.
- Do not click on the malicious link.
- Apply filter to accept only trusted HTTPS connection.
- Use anti-proxy techniques to avoid malicious IP sources.
- Disallow the communication feature for unknown connection.
- Do not install unwanted application from untrusted source.
- Do not use malicious/free VPN to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.
- Enable limitations on administrative access or rights.

Remediation

- Download only trusted software from known sites.
- Use post method for sending & retrieving of data through communication channel.
- Update your machine & servers on monthly basis.
- Enable packet filtration through firewall.
- Update the operating system (OS) and all programs installed programs.
- Use paid VPN to access the web applications or network.
- Use trusted anti-malware & anti-phishing programs.

TOP THREAT ACTORS

Threat Actor	IOC Reference
Lockbit	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
Volt Typhoon	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
Moveit	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
Zero-Day ManageEngine ADSelfService Plus GINA Client Insufficient Verification of Data Authenticity Authentication Bypass Vulnerability CVE-2023-35719	Vulnerability allows physically present attackers to execute arbitrary code on affected installations of ManageEngine ADSelfService Plus. The issue results from the lack of proper authentication of data received via HTTP.	VDB-232104 | VulDB
(Pwn2Own) Microsoft Windows UMPDDrvEnablePDEV Improper Input Validation Local Privilege Escalation Vulnerability CVE-2023-29539	Vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system to exploit this vulnerability.	ZDI-23-890 | Zero Day Initiative
(Pwn2Own) Microsoft SharePoint ValidateTokenIssuer Improper Verification of Cryptographic Signature Authentication Bypass Vulnerability CVE-2023-29357	Vulnerability allows remote attackers to bypass authentication on affected installations of Microsoft SharePoint.The specific flaw exists within the ValidateTokenIssuer method.	Microsoft SharePoint Server Elevation of Privilege Vulnerability | MSRC
(Pwn2Own) Western Digital MyCloud PR4100 do_reboot Command Injection Remote Code Execution Vulnerability CVE-2022-29841	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Western Digital MyCloud PR4100 NAS devices. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed.	WDC-23002 | Western Digital
(Pwn2Own) Samsung Galaxy S22 McsWebViewActivity Permissive List of Allowed Inputs Remote Code Execution Vulnerability CVE-2023-21516	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Samsung Galaxy S22 smartphones. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	SVE-2023-0136 | Samsung Mobile Security
VMware Aria Operations for Networks createSupportBundle Command Injection Remote Code Execution Vulnerability CVE-2023-20887	Vulnerability allows remote attackers to execute arbitrary code on affected installations of VMware Aria Operations for Networks.The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call.	VMSA-2023-0012.2 | vmware
NETGEAR RAX30 cmsCli_authenticate Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-34285	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR RAX30 routers. The specific flaw exists within a shared library used by the telnetd service, which listens on TCP port 23 by default.	RAX30 Firmware Version 1.0.11.96 - Hot Fix | NETGEAR
Unified Automation UaGateway NodeManagerOpcUa Use-After-Free Remote Code Execution Vulnerability CVE-2023-32174	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Unified Automation UaGateway. Authentication is required to exploit this vulnerability when the product is in its default configuration. The specific flaw exists within the handling of NodeManagerOpcUa objects.	Multiple vulnerabilities in Unified Automation UaGateway | Cybersecurity Help

Security Bulletin

1. Ransomware group used MOVEit exploit to steal data from dozens of organizations

- Recently MOVEit zero-day attack was connected with a known ransomware group that had been exploiting the vulnerability to steal the data from many organizations.
- Progress software conveyed to it's customers on May 31 that its MOVEit transfer managed file transfer (MFT) software is affected by the critical SQL injection vulnerability that can be exploited by an unauthenticated attacker to access databases associated with their product.
- The CVE identifier CVE-2023-34362 has been assigned to this flaw, which has been patched with the release of versions 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5) and 2023.0.1 (15.0.1). MOVEit Cloud was also impacted, but there was a fix been deployed and no action is required by the users.
- Many cybersecurity organizations have reported looking over attacks involving the MOVEit zero-day, including Huntress, Rapid7, TrustedSec, GreyNoise, Mandiant, and Volexity. Mandiant had reported the first of the attacks on May 27, but threat intelligence firm GreyNoise observed scanning activity possibly related to this flaw in early March. In the observed attacks, threat actors have exploited the vulnerability to create and access the webshell/ backdoor that allows them to steal data uploaded by MOVEit Transfer end users.
- Mandiant has attributed the attack to UNC4857, a new threat cluster, and named the delivered webshell LemurLoot. The security firm has seen victims in the US, Canada and India, with data theft occurring within minutes of the webshell deployment in some cases. Mandiant said, "The seemingly opportunistic nature of this campaign and subsequent data theft activity is consistent with activity that we've seen from extortion actors, which means victim organizations could potentially receive ransom emails in the coming days to weeks."
- The Shodan search engine shows around 2,500 internet-exposed MOVEit systems, mostly located in United States. The Censys search engine has found more than around 3,000 hosts, including in the financial, education and government sectors. Security researcher **Kevin Beaumont**, had been analyzing the cyberattacks, is aware of data being stolen from a 'double digit number' of organizations, including financial companies and US government agencies. The US Cybersecurity and Infrastructure Security Agency (CISA) has added CVE-2023-34362 to its Known Exploited Vulnerabilities Catalog, instructing government agencies to patch it as soon as possible.

2. Cybercriminals exploit legitimate websites for credit card theft

- Security experts recently discovered a new Magecart campaign aimed at stealing personal PII and credit card info from e-commerce websites. Around the world, including in Europe, Latin America, and North America, Akamai has identified victims on various scales.Threat actors build their C2 infrastructure as part of this new campaign, which is distinct in that they usually exploit well-known vulnerabilities to do so.
- Within the starting stage of operation, the aggressors distinguish defenseless genuine websites, which they hack into. These compromised websites then serve as their C2 servers.
    - By leveraging trustworthy websites, the aggressors cleverly dodge location and circumvent blocks, eliminating the need to set up their own foundation.
    - In this way, the assailants continue to infuse a brief JavaScript snippet into their focused e-commerce sites. This snippet recovers malevolent code from the already compromised websites.
- Encryption for stealthiness
    - To further elevate the stealthiness of their assault, the assailants have utilized Base64 encoding to muddle the credit card skimmer.
    - This encoding procedure not only conceals the URL of the host but also embraces a structure which takes after that of well-known third-party services such as Google Tag Manager or Facebook Pixel.

- Why this matters
    - This campaign fundamentally centres on focusing on commerce organizations, and the sheer magnitude of the assault is noteworthy. A few victim organizations get a monthly inflow of hundreds of thousands of guests.
    - Subsequently, this puts thousands, and possibly tens of thousands, of people at hazard of having their credit card information and PII stolen.
    - Web skimming assaults deal considerable damage to e-commerce organizations. The consequences can be hindering, leading to reputational harm and other antagonistic results.
- Attacks get worse
    - It's worth noticing that various high-profile Magecart assaults go undetected for months or even longer.
    - In 2022 alone, out of 9,290 e-commerce spaces influenced by Magecart assaults, a stunning 2,468 remained effectively tainted until the year's conclusion, underscoring the imposing danger postured to commerce organizations
- Wrap up
    - This campaign serves as an update that web skimming remains an inescapable security danger. Malevolent artists continually adjust their strategies to jumble their exercises and make discovery more strenuous. Conventional inactive examination instruments fall short in combating web skimmers, as aggressors ceaselessly alter their approaches and utilize progressively modern strategies, making them capable at avoiding inactive investigation strategies.

3. SpinOk Android malware found in more apps with 30 million installs

- The SpinOk malware was found in a modern batch of Android apps on Google Play, supposedly downloaded an extra 30 million times. The finding comes from CloudSEK's security group, who report finding a set of 193 apps carrying the malevolent SDK, 43 of which were still on Google Play at the time of their disclosure final week.
- SpinOk was first discovered by Dr. Web late last month in a set of a hundred apps that had been collectively downloaded over 421 million times. As the mobile security company clarified in its report, SpinOk was conveyed through an SDK supply chain assault that contaminated numerous apps and, by expansion, breached numerous Android users. On the surface, the SDK served mini-games with everyday rewards authentically utilized by engineers to provoke the intrigue of their clients. In any case, within the background, the trojan may well be utilized to take records and switch clipboard substance. CloudSEK utilized the IoCs given in Dr.Web's report to reveal more SpinOk contamination, expanding the list of corrupt apps to 193 after finding an extra 92 apps. Nearly half of those were accessible on Google Play.
- The most downloaded of the new set was HexaPop Link 2248, which had 5 million downloads. Be that as it may, it has been expunged from Google Play since CloudSEK compiled its report. Other prevalent apps utilizing the SpinOk SDK and which stay accessible for download by means of Google Play are:
    - Happy 2048 (Zhinuo Technology) – 1 million downloads
    - Macaron Match (XM Studio) – 1 million downloads
    - Crazy Magic Ball (XM Studio) – 1 million downloads
    - Jelly Connect (Bling Game) – 1 million downloads
    - Tiler Master (Zhinuo Technology) – 1 million downloads
    - Macaron Boom (XM Studio) – 1 million downloads
    - Mega Win Slots (Jia22) – 500,000 downloads
- CloudSEK reports that the collective download number for the extra SpinOK-ridden apps comes to over 30,000,000. It ought to be famous that the designers of these apps likely utilized the noxious SDK considering it was a promoting library, uninformed that it included malignant usefulness.

4. New PowerDrop malware targets U.S. aerospace industry

- A new malware called PowerDrop, which targets the aviation sector in the U.S., has just been detected by Adlumin and was reported to be an unknown threat actor using PowerShell. In order to prevent detection, they employed advanced techniques such as deception, encoding and encryption. In May, researchers discovered this malware in an unidentified domestic aerospace defence contractor.
- Malware Analysis
    - The researchers determined that the malware contained a new combination of PowerShell and Windows Management Instrumentation, which was designed to be RAT with persistence.
    - The malware is able to use echo request messages sent via Internet Control Message Protocol, ICMP, as a trigger for its C2 functionality.
    - For data exfiltration applications, complementary ICMP ping techniques can also be used.
    - Overall, it appears that after successful intercepting, implementing, and maintaining persistence on servers, the main goal of the Trojan is to carry out remotely controlled commands within targeted networks.
- Why this matters
    - The recent attacks have highlighted the advances of techniques used by potential enemies, such as living off the land.
    - While the use of PowerShell for remote access and WMI-based persistence of PowerShell scripts, as well as ICMP triggering and tunnelling, are not novel concepts, this malware presents a unique combination that hasn't been observed previously.
    - It has a position among the basic, run-of-the-mill threats and sophisticated tactics commonly used by APT groups.
- Although it does not yet have an extremely advanced structure, the ability to conceal suspicious activity and circumvent a defence against endpoints suggest that more sophisticated threat actors are involved.

5. Latest PowerShell threats

- A refined PowerShell script has been devised by the Vice Society ransomware group to take advantage of infected networks and automate data theft. The plot uses what is called "Living-off-the-land" techniques to evade detection by security software, which makes it more difficult for defenders to fight off their attacks.
- In April, assailants were found using password-protected WinRAR self-extracting (SFX) archives to install persistent backdoors in target systems undetected. Using customized SFX archives, they are allowed to run PowerShell and other ill intent scripts that don't trigger the security agent.
- **The End Note**
    - Adlumin advises people in the aeronautics defense industry to maintain a high degree of awareness about PowerDrop. In order to detect unusual pinging originating in their networks towards external resources, the company recommends performing vulnerability scans on Windows systems and maintaining a high level of vigilance. The power to blend old and new technologies within a modern landscape is demonstrated by the PowerDrop malware.

6. Spanish bank Globalcaja hit by ransomware attack

- Spanish bank Globalcaja confirmed on Friday that it had suffered a cyber-incident in which the ransomware attack was carried out against some of its own local systems. A group calling itself "Play ransomware" claims to be behind the attack. According to the company's official statement, which was published on Twitterin Spanish, the attack took place last Thursday and forced the financial institution to activate its security protocols.
- Globalcaja reassured customers that no customer accounts or agreements were compromised by the ransomware attack, nor was the normal functioning of its electronic banking platform Ruralva affected.
- Additionally, the company confirms that customers are able to carry out their financial transactions safely via

Internet Banking and have access to a number of ATMs free of charge. In order to contain the problem and minimise its potential effects, Globalcaja implemented a temporary suspension of some office workstations in their preventive measures.

- Rebecca Moody, chief data analyst at Comparitech, says that this year there has been an increase in significant headline attacks on finance institutions. Notable incidents include a cyber-attack on Tri Counties Bank in the US, which was later claimed by BlackBasta, an attack on Latitude Financial in Australia that potentially compromised around 14 million records, and the LockBit attacks on Fullerton India (demanding a $3m ransom) and Bank Syariah Indonesia (with a demand of $20m). “As we can see with this latest case against Globalcaja, attacks on these types of organizations are of particular concern due to the highly sensitive data they hold,” Moody added. “Although financial institutions should be applauded for refusing to comply with hackers’ demands, they must also make it easy for their customers to take all the necessary steps in order to prevent identity theft and other types of fraud”.

REFERENCE LINKS

1. https://www.securityweek.com/ransomware-group-used-moveit-exploit-to-steal-data-from-dozens-of-organizations/?web_view=true
2. https://cyware.com/news/cybercriminals-exploit-legitimate-websites-for-credit-card-theft-a25e3959
3. https://www.bleepingcomputer.com/news/security/spinok-android-malware-found-in-more-apps-with-30-million-installs/?&web_view=true
4. https://cyware.com/news/new-powerdrop-malware-targets-us-aerospace-industry-146aa0d1
5. https://www.infosecurity-magazine.com/news/spanish-bank-globalcaja-hit/
6. https://www.csoonline.com/article/3700572/apple-patches-exploits-used-in-spy-campaign-operation-triangulation.html
7. https://www.csoonline.com/article/3700488/ransomware-attacks-pose-communications-dilemmas-for-local-governments.html
8. https://www.csoonline.com/article/3700170/romanian-cybercrime-gang-diicot-builds-ddos-botnet-with-mirai-variant.html
9. https://www.csoonline.com/article/3700169/trend-micro-adds-generative-ai-to-vision-one-for-enhanced-xdr.html
10. https://www.csoonline.com/article/3700488/ransomware-attacks-pose-communications-dilemmas-for-local-governments.html
11. https://www.csoonline.com/article/3700849/millions-of-github-repositories-vulnerable-to-repojacking-report.html
12. https://www.bleepingcomputer.com/news/security/asylum-ambuscade-hackers-mix-cybercrime-with-espionage/
13. https://www.darkreading.com/threat-intelligence/asylum-ambuscade-cyberattackers-financial-cyber-espionage
14. https://thehackernews.com/2023/06/microsoft-warns-of-widescale-credential.html
15. https://latesthackingnews.com/2023/06/26/serious-idor-vulnerability-found-in-microsoft-teams/
16. https://thehackernews.com/2023/06/experts-uncover-year-long-cyber-attack.html
17. https://www.oodaloop.com/cyber/2023/06/26/microsoft-warns-of-widescale-credential-stealing-attacks-by-russian-hackers/

About SDG

SDG is a global cybersecurity, identity governance, GRC, risk consulting and advisory firm. SDG's SaaS platform TruOps in combination with its services deliver a comprehensive range of identity, cybersecurity, risk, compliance, and cloud security solutions that enable organizations to identify and mitigate cyber risk, protect cyber assets, and manage their business securely.

To learn how SDG can help ensure the security and compliance of your technology and data infrastructure visit **www.sdgc.com** and **www.truops.com**.

SDG

55 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com