Cyber Threat Advisory

APRIL 2023

Contents

Monthly Highlights - April

1. **Massive data breach unearthed in India exposing sensitive data of 16.8 crore of its citizens as well as personnel of Defence and other important organizations**

   A massive data breach has been identified by authorities in India after arresting seven people of a gang allegedly involved in the theft and sale of sensitive data of the government and important organisations, including details of defence personnel as well as the personal and confidential data of about 16.8 crore citizens. The gang was selling this sensitive data to cybercriminals via three different companies in Noida and consisted of more than 140 different categories of information obtained and aggregated through various data breaches.

2. **Most mid-sized businesses in US and Canada are facing cybersecurity challenges with no dedicated cybersecurity experts or incident response plans**

   As per a recent report, 61% of mid-sized businesses in the United States and Canada do not have a dedicated cybersecurity expert, while 47% of respondents in the survey reported their organization does not currently have an incident response plan, putting their organization at a severe disadvantage for quickly and effectively dealing with security incidents when they occur. The report also highlighted that 24% of mid-sized businesses have suffered a cyberattack or are unsure if they have suffered a cyber-attack in the last twelve months while 27% of organizations reported having no cyber insurance coverage.

3. **Lionsgate – a popular entertainment company suffers from data leak exposing 37M subscriber data of its application Lionsgate play**

   Lionsgate Entertainment Corporation, the Canadian American entertainment company operating the platform that owns several well-known movie and TV franchises like Twilight Saga and Terminator was found to be accidently leaking data of 37M subscribers of its movie streaming platform Lionsgate Play due to an open Elasticsearch instance. The exposed subscriber data consisted of IP addresses and user data concerning device, operating system, and web browser as well as platform's usage data and unidentified hashes.

4. **Business Email Compromise (BEC) replaces ransomware as the top cybercrime activity**

   Business Email Compromise doubled in volume in the year 2022 and accounted for a third (33%) of initial access vectors – up from 13% in 2021. At the same time, ransomware

fell from its top spot as the most common cybercrime type with detections declining by 57% as the threat actors could be targeting smaller organizations which are less likely to engage incident responders. As per the recently observed trends, ransomware groups will increasingly look to adopt other criminal models that monetize initial access, like BEC.

5. **Microsoft Outlook Vulnerability CVE-2023-23397 being referred as 'Bug of the Year' by security experts**

   A recently patched zero-day vulnerability in Microsoft Outlook is under active exploitation. Identified as CVE-2023-23397, it can enable an attacker to perform a privilege escalation, accessing the victim's Net-NTLMv2 challenge-response authentication hash and impersonating the user.

   This critical bug affects those running an Exchange server and the Outlook for Windows desktop client while Outlook for Android, iOS, Mac, and Outlook for Web (OWA) are unaffected.

   The attack surface affects almost everyone (small to large enterprises) and is at least as big as the user base of desktop Outlook, and potentially core IT systems connected to Windows 365, and even any recipients of emails sent through Outlook.

   The vulnerability can be exploited by external attackers over email, and the target doesn't even have to open the email to fall victim to an attack.

   > **Remedial Action:** Apply the appropriate Microsoft patch for the vulnerability. For organizations unable to patch right away, administrators should block TCP 445/SMB outbound traffic to the Internet from the network using perimeter firewalls, local firewalls, and VPN settings. Please see our 'Top Exploitable Vulnerabilities' section below for detailed links.

6. **Zero-day vulnerabilities in edge infrastructure products being probed the most by attackers**

   As per a report associated with zero-day attacks in 2022, threat actors are increasingly probing for security weaknesses in edge-infrastructure technologies, including VPNs, firewalls, and IT management products.

   Among them were CVE-2022-1040 and CVE-2022-3236 in Sophos firewalls, CVE-2022-20821 in Cisco IOS, CVE-2022-42474 and CVE-2022-41226 in Fortinet's FortiOS, CVE-2022-288810 in Zoho ManageEngine, and CVE-2022-35247 in SolarWinds Serv-u.

   Chinese threat actors continue to be the most active exploiters of the zero-days as per the analysis.

7. **Managing third party risks should be a top cybersecurity concern**

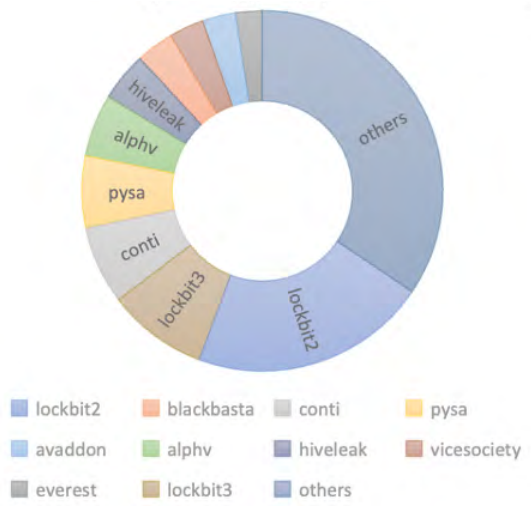
   With the rise in digital transformation, more data is being shared outside the perimeter of an organization with weak visibility of that data. In such a scenario, even a single third-party data breach can prove to be catastrophic for the organization of any size.

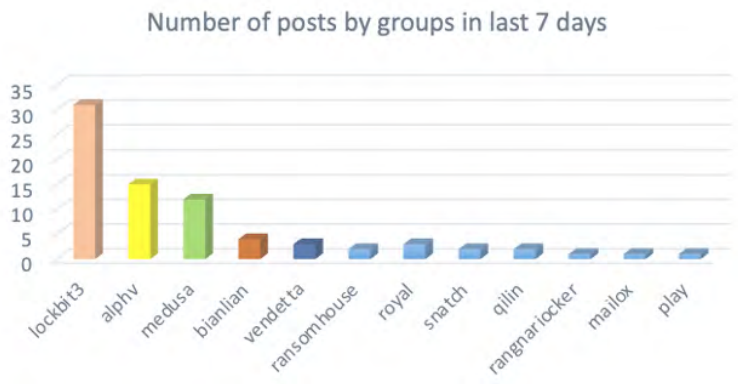
   It is to be noted that 60% of all data breaches are initiated via third-party vendors, which are often undetectable by the usual outward-facing approach to security until they have reached the perimeter of an organization.

   In order to be effective in today's scenario, a third-party risk strategy must be pre-emptive. Reviewing security policies, understanding their dedication to visibility, and having strong security hygiene is important before committing to share data with them. Part of this evaluation should be implementing contracts for existing partnerships with clawback clauses to deal with failure to comply with security standards and integrating supply chain penalties for data leaks of confidential information.

   From there, it's important to maintain that pre-emptive security posture through ongoing monitoring and risk assessment. Automated risk management platforms, regular real-time risk assessments, and tools (such as external attack surface management, or EASM) for continually discovering, inventorying, classifying, prioritizing, and monitoring sensitive external assets within an IT infrastructure are very helpful as a part of a larger third-party life cycle management plan.

Ransomware Engagement Tracker





Stop Ransomware: Royal Ransomware

The ransomware operation uses unusual techniques to breach networks before encrypting them with malware and demanding ransom payments. Some Royal ransomware campaigns distribute the malware via malicious attachments, and some distribute the malware via malicious advertisements.

Although Royal is a newer ransomware operation, researchers believe the threat actors behind it are very experienced due to evidence of previously seen tactics and techniques. Let's take a look at Royal, their tactics and techniques, and what organizations can do to protect themselves and keep their cyber environments safe.

Detection:

- Royal actors gain initial access to victim networks in several ways, including phishing. According to third-party reporting, Royal actors most commonly (in 66.7% of incidents) gain initial access to victim networks via successful phishing emails [T1566]. According to open-source reporting, victims have unknowingly installed malware that delivers Royal ransomware after receiving phishing emails containing malicious PDF documents [T1566.001], and malvertising [T1566.002]. Remote Desktop Protocol (RDP). The second most common vector Royal actors use (in 13.3% of incidents) for initial access is RDP compromise public-facing applications. FBI has also observed Royal actors gain initial access through exploiting public-facing applications [T1190]. Another common vector Royal actors use is brokers. Reports from trusted third-party sources indicate that Royal actors may leverage brokers to gain initial access and source traffic by harvesting virtual private network (VPN) credentials from stealer logs.

Command and Control

Once Royal actors gain access to the network, they communicate with command and control (C2) infrastructure and download multiple tools [T1105]. Legitimate Windows software is repurposed by Royal operators to strengthen their foothold in the victim's network. Ransomware operators often use open-source projects to aid their intrusion activities; Royal operators have recently been observed using Chisel, a tunnelling tool transported over HTTP and secured via SSH [T1572], to communicate with their C2 infrastructure. FBI has observed multiple Qakbot C2s used in Royal ransomware attacks but has not yet determined if Royal ransomware exclusively uses Qakbot C2s.

Lateral Movement and Persistence

Royal actors often use RDP to move laterally across the network [T1021.001]. Microsoft Sysinternals tool PsExec has also been used to aid lateral movement. FBI has observed Royal actors using remote monitoring and management (RMM) software, such as AnyDesk, LogMeIn, and Atera, for persistence in the victim's network [T1133]. In some instances, the actors moved laterally to the domain controller. In one confirmed case, the actors used a legitimate admin account to remotely.log on to the domain controller [T1078]. Once on the domain controller, the threat actor deactivated antivirus protocols [T1562.001] by modifying Group Policy Objects [T1484.001].

Exfiltration

Royal actors' exfiltrate data from victim networks by repurposing legitimate cyber pentesting tools, such as Cobalt Strike, and malware tools and derivatives, such as Ursnif/Gozi, for data aggregation and exfiltration. According to third-party reporting, Royal actors' first hop in exfiltration and other operations is usually a U.S. IP address. Note: In reference to Cobalt Strike and other tools mentioned above, a tool repository used by Royal was identified at IP: 94.232.41[.]105 in December 2022.

Encryption

Before starting the encryption process, Royal actors:

- Use Windows Restart Manager to determine whether targeted files are currently in use or blocked by other applications [T1486].
- Use Windows Volume Shadow Copy service (vssadmin.exe) to delete shadow copies to inhibit system recovery.

FBI has found numerous batch (.bat) files on impacted systems which are typically transferred as an encrypted 7zip file. Batch files create a new admin user [T1078.002], force a group policy update, set pertinent registry keys to auto-extract [T1119] and execute the ransomware, monitor the encryption process, and delete files upon completion—including Application, System, and Security event logs [T1070.001].

Malicious files have been found in victim networks in the following directories:

- C:\Temp\
- C:\Users\\AppData\Roaming\
- C:\Users\\
- C:\ProgramData\ Indicators of Compromise (IOC)

Royal ransomware IOCs that FBI obtained during threat response activities as of some of the observed IP addresses are several months old. FBI and CISA recommend vetting or investigating these IP addresses prior to taking forward-looking action, such as blocking.

Table 1: Royal Ransomware Associated Files

IOC	Description
.royal	Encrypted file extension
README.TXT	Ransom note

Table 2: Domain and IP addresses

Malicious IP	Malicious Domain
102.157.44[.]105	ciborkumari[.]xyz
105.158.118[.]241	sombrat[.]com
105.69.155[.]85	gororama[.]com
113.169.187[.]159	softeruplive[.]com
134.35.9[.]209	altocloudzone[.]live
139.195.43[.]166	ciborkumari[.]xyz

Table 3: Tools used by Royal operators

Tool	SHA256
AV Tamper	8A983042278BC5897DBCDD54D1D7E3143F8B7EAD553B5A4713E30DEFFDA16375
TCP/UDP Tunnel over HTTP (Chisel)	8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451
Ursnif/Gozi	be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1
Exfil	B8C4AEC31C134ADBDBE8AAD65D2BCB21CFE62D299696A23ADD9AA1DE082C6E20
Remote Access (AnyDesk)	4a9dde3979c2343c024c6eeeddff7639be301826dd637c006074e04a1e4e9fe7
Ransomware Executable	d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681

- Exploit Public Facing (Application T1190) | The actors gain initial access through public- facing applications.
- Phishing: Spear phishing (Attachment T1566.001) | The actors gain initial access through malicious PDF attachments sent via email.
- Phishing: Spear phishing Link (T1566.002) | The actors gain initial access using malvertising links via emails and public-facing sites.
- External Remote Services (T1133) | The actors gain initial access through a variety of RMM software.
- Ingress Tool Transfer (T1105) | The actors used C2 infrastructure to download multiple tools.
- Protocol Tunnelling (T1572) | The actors used an encrypted SSH tunnels to communicate within C2 infrastructure.
- Valid accounts: Domain Accounts (T1078.002) | The actors used encrypted files to create new admin user accounts.
- Impair Defences: Disable or Modify Tools (T1562.001) | The actor deactivated antivirus protocols.
- Domain policy modification: Group policy modification (T1484.001) | The actors modified group policy objects to subvert antivirus protocols.
- Indicator Removal: Clear Windows Event Logs (T1070.001) | The actors deleted shadow files and system and security logs after exfiltration.
- Remote Desktop Protocol (T1021.001) | The actors used valid accounts to move laterally through the domain controller using RDP.
- Automated Collection (T1119) | The actors used registry keys to auto-extract and collect files.
- Data Encrypted for Impact (T1486) | The actors encrypted data to determine which files were being used or blocked by other applications.

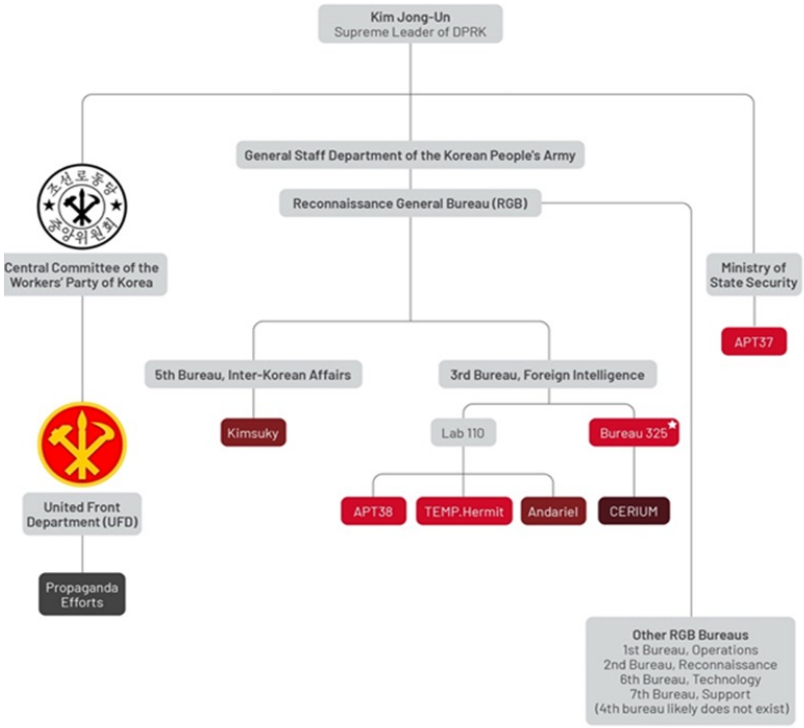
Prevention:

- Do not download untrusted software's from unknown sites.
- Update the operating system (OS) and all programs installed programs.
- Always check latest patch update on software and other application.
- Always take backups in different locations on daily basis.
- Avoid using remote desktop servers.
- Develop defence systems.
- Use multi-factor authorization.

Remediation:

- Use XDR implement for monthly updates.
- Implement endpoint detection procedures.
- Use antivirus/anti-malwares programs.
- Update endpoints on weekly/monthly basis.
- Enable packet filtration procedures.
- Implement IDS/IPS techniques.
- Enable BC/DR method for taking server backups.
- Create checklist for ransomware on monthly bases.
- Implement incident response team.

Reference Link: #StopRansomware: Royal Ransomware | CISA



New UNC2970 Espionage Campaign Targets Media and Tech Companies

The North Korean cyberespionage group UNC2970 who has been targeting media and tech companies in the U.S. and Europe reveals Mandiant. The group carries out delivers a plethora of new malicious tools via spear phishing attacks. As noted by experts, its TTPs are consistent with several other North Korean espionage groups.

LIDSHOT sends the following information back to its C2:

- Computer Name
- Product name as recorded in the following registry key SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\ProductName
- IP address
- Process List with User and Session ID associate per process

Phishing via fake job schemes

According to Mandiant researchers, UNC2970 specifically targets security researchers of an enterprise using a job recruitment theme.

- The attackers create fake accounts on LinkedIn, posing as professional recruiters. These accounts are used to approach the targeted victims and socially engineer them into having a WhatsApp conversation.
- During the conversation, attackers deliver a malicious payload, primarily Word documents claiming to be a job description, directly via WhatsApp or email.

Detection:

- To establish a foothold, UNC2970 deploys PLANKWALK, a C++ backdoor, executed through a launcher. The backdoor further allows attackers to distribute additional tools on the target machine.
- PLANKWALK communicates with the C2 server (mostly compromised WordPress sites) and then leverages a wide variety of additional tooling, including TOUCHSHIFT (a malware dropper), TOUCHSHOT (screenshot grabber), TOUCHKEY (keylogger), HOOKSHOT (a TCP tunnelling tool), TOUCHMOVE (a loader), and SIDESHOW (C/C++ backdoor) to gather intelligence.
- It abuses Microsoft Intune to upload custom PowerShell scripts containing malicious code to be deployed, including CLOUDBURST (a C-based backdoor).
- The attack continues further with an in-memory-only dropper called LIGHTSHIFT. This dropper drops the LIGHTSHOW utility, which uses anti-analysis techniques to hinder both static and dynamic analysis.

Prevention:

- Do not download untrusted sites.
- Update the operating system (OS) and all programs installed programs.
- Always check latest patch update on software and other applications.
- Always take backups in different locations on daily basis.
- Avoid using remote desktop servers.
- Develop defence systems.
- Use multi-factor authorization.

Remediation:

- Use XDR implement for monthly updates.
- Implement endpoint detection procedures.
- Use antivirus/anti-malwares program.
- Update Endpoints on weekly/monthly basis.
- Enable packet filtration procedures.
- Implement IDS/IPS techniques.
- Enable BC/DR method for taking server backups.
- Create checklist for ransomware on monthly bases.
- Implement incident response teams.

Reference Link: Stealing the LIGHTSHOW (Part One) — North Korea's UNC2970 | Mandiant

IOC	Signature
e97b13b7e91edecee ac876c3869cc4eb	PLANKWALK
a9e30c16df400c3f24 fc4e9d76db78ef	PLANKWALK
f910ffb063abe31e87 982bad68fd0d87	PLANKWALK
30358639af2ecc217b bc26008c5640a7	LIDSHIFT
41dcd8db437157445 3561251701107bc	LIDSHOT
866f9f205fa1d47af27 173b5eb464363	TOUCHSHIFT
8c597659ede15d9791 4cb27512a55fc7	TOUCHSHIFT
a2109276dc704dedf 481a4f6c8914c6e	TOUCHSHIFT

TOUCHSHIFT - A malware dropper that loads follow-on malware ranging from keyloggers and screenshot utilities to full-featured backdoors.

TOUCHSHOT - A software that configured to take a screenshot every three seconds.

TOUCHKEY - A keylogger that captures keystrokes and clipboard data.

HOOKSHOT - A tunnelling tool that connects over TCP to communicate with the command-and-control (C2) server.

TOUCHMOVE - A loader that's designed to decrypt and execute a payload on the machine.

SIDESHOW - A C/C++ backdoor that runs arbitrary commands and communicates via HTTP POST requests with its C2 server.

The activities of the UNC2970 group have been linked, with high confidence, to the UNC577 group (aka Temp Hermit), one of the sub-groups working under the Lazarus collective.

Spear-phishing attacks leveraging a job-recruitment theme via fake LinkedIn profiles have some overlaps with Operation Dream Job that has been tracked and reported by several agencies including Clear sky, Google, and Proof point.

Talos Uncovers Espionage Campaigns Targeting CIS Countries, Embassies and EU Health Care Agency

- Cisco Talos has identified a new threat actor, naming "Yoro Trooper," that has been running several successful espionage campaigns since June 2022.
- Based on analysis Yoro Trooper's main targets are government or energy organizations in Azerbaijan, Tajikistan, Kyrgyzstan and other Commonwealth of Independent States (CIS).
- Yoro Trooper compromise accounts from at least two international organizations, which is critical named European Union (EU) health care agency and the World Intellectual Property Organization (WIPO).

About Yoro Trooper

- This new threat actor we are naming "Yoro Trooper" has been targeting governments across Eastern Europe since at least June 2022, and Cisco Talos has found three different activity clusters with overlapping infrastructure that are all linked to the same threat actor.
- Cisco Talos does not have a full overview of this threat actor, as we were able to collect varying amounts of detail in each campaign.

Detection

- Yoro Trooper's main tools include Python-based, custom-built, and open-source information stealers, such as the Stink stealer wrapped into executables via the Nuitka framework and PyInstaller.
- Yoro Trooper has also deployed commodity malware, such as AveMaria/Warzone RAT, LodaRAT and Meterpreter for remote access.
- The infection chain consists of malicious shortcut files (LNKs) and optional decoy documents wrapped in malicious archives delivered to targets.
- Information stolen from successful compromises include credentials from multiple applications, browser histories & cookies, system information and screenshots.

Attacking Procedure

- During the assessment operators of this threat actor are Russian language speakers, but not necessarily living in Russia or Russian nationals since their victimology consists mostly of countries in the Commonwealth of Independent States (CIS).
- There are also snippets of Cyrillic in some of their implants, indicating that the actor is familiar with the language.
- The threat actor either registers malicious domains and then generates subdomains or registers typo-squatted domains which is like legitimate domains from CIS entities to host malicious artifacts.

MALICIOUS SUBDOMAIN	LEGITIMATE DOMAIN	ENTITY
mail[.]mfa[.]gov[.]kg[.]openingfile[.]net	mfa[.]gov[.]kg	Kyrgyzstan's Ministry of Foreign Affairs
akipress[.]news	akipress[.]com	AKI Press News Agency (Kyrgyzstan-based)
maileecommission[.]inro[.]link	commission[.]europa[.]eu	European Commission's email
sts[.]mfa[.]gov[.]tr[.]mypolicy[.]top	mfa[.]gov[.]tr	Turkey's Ministry of Foreign Affairs
industry[.]tj[.]mypolicy[.]top	industry[.]tj	Tajikistan's Ministry of Industry and New Technologies
mail[.]mfa[.]az-link[.]email	mail[.]mfa[.]az	Azerbaijan's Ministry of Foreign Affairs
belaes[.]by[.]authentication[.]becloud[.]cc	belaes[.]by	Belarusian Nuclear Power Plant (Astravets)
belstat[.]gov[.]by[.]attachment-posts[.]cc	belstat[.]gov[.]by	National Statistical Committee of Belarus
minsk[.]gov[.]by[.]attachment-posts[.]cc	minsk[.]gov[.]by	Official Website of the Government of Minsk (Belarus)

ACTOR PROFILE

YoroTrooper

Affiliations

Unknown

Active Since

2022

Goals

Espionage, data theft

Victimology

European Union, World Intellectual Property Organization, Turkey and CIS countries, Energy and government sectors.

Notable TTPs

Social Engineering, spear-phishing, data exfiltration, custom malware and commodity malware.

Malware & tooling

YoroTrooper employs a variety of self-developed and commodity malware families, such as AveMaria/Warzone RAT, LodaRAT.

Prevention

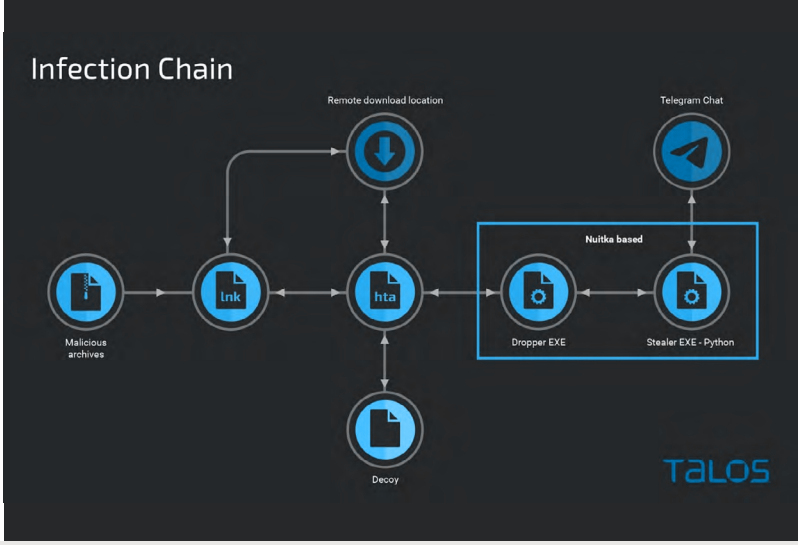
- Prevent with Yoro Trooper's payload legitimate process which is used to install malicious malware.
- Use Anti-Cyrillic word techniques for domain detection.
- Do not click on the malicious link.
- Do not click on the spam & suspicious phishing emails.
- Do not use malicious/free VPN to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.

Remediation

- Download only trusted software's from known sites.
- Use post method for sending & retrieving of data.
- Use domain verification through SPF.
- Update your machine & servers on monthly basis.
- Enable packet filtration through the 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 programs.

Attacking Procedure (Continued)

- The initial attack vectors are phishing emails with a file attached, which usually consists of an archive consisting of two files: a shortcut file and a decoy PDF file.
- The shortcut file is the initial trigger for the infection, while the PDF is the lure to make the infection look legitimate.
- The latest infection chain from January 2023 is relatively straightforward but consists of multiple components such as archives, LNKs, HTAs and ultimately the final payloads.



Tick APT Targeted High-Value Customers of East Asian Data-Loss Prevention Company

- A new malware campaign targeting an East Asian company that develops data-loss prevention (DLP) software for government and military entities has been attributed to the advanced persistent threat (APT) group known as Tick.
- The threat actor breached the DLP company's internal update servers to deliver malware within its network.
- Attacker used Trepanised installer which eventually result in execution of malware on the computers of the company's customers.
- Tick, also known as Bronze Butler, REDBALDKNIGHT, Stalker Panda, and Stalker Taurus, is a suspected China-aligned collective that has primarily gone after government, manufacturing, and biotechnology firms in Japan.

Detection

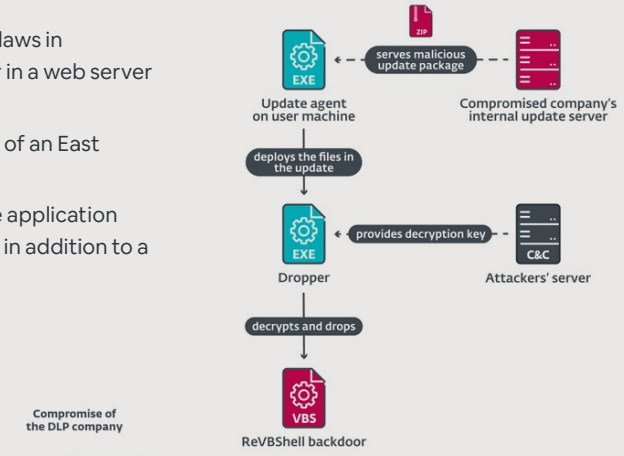
- The attackers deployed a previously undocumented downloader named ShadowPy, and they also deployed the Netboy backdoor and Ghostdown downloader.
- The attackers installed support tools to transfer the trojanized installers themselves.
- The group maintained persistent access by deploying malicious loader DLLs, along with legitimate signed applications vulnerable to DLL search order hijacking.
- Tick emerged as one of the threat actors to capitalize on the ProxyLogon flaws in Microsoft Exchange Server as a zero-day to drop a Delphi-based backdoor in a web server belonging to a South Korean IT company.
- The adversarial collective is believed to have gained access to the network of an East Asian software developer company through unknown means.
- This was followed by the deployment of a tampered version of a legitimate application called Q-Dir to drop an open-source VBScript backdoor named ReVBShell, in addition to a previously undocumented downloader named ShadowPy.
- ShadowPy, as the name indicates, is a Python downloader that's responsible for executing a Python script retrieved from a remote server.
- During the intrusion were variants of a Delphi backdoor called Netboy that comes with information gathering and reverse shell capabilities as well as another downloader codenamed Ghostdown.
- To maintain persistent access, the attackers deployed malicious loader DLLs along with legitimate signed applications vulnerable to DLL search-order hijacking.

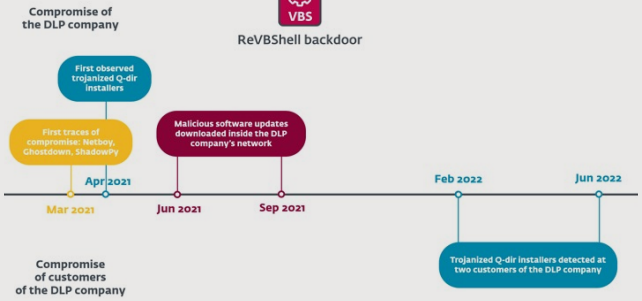
Prevention

- Block unknown VBScripts & batch scripts.
- Patch all DLL files in production.
- Do not click on the malicious link.
- Disallow the RDP feature for unknown connection.
- Do not use malicious/free VPN to access the web applications or network.
- Implement packet filtration & IDS/IPD mechanism through the firewall.

Remediation

- Download only trusted software's from known sites.
- Use post method for sending & retrieving of data.
- 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 programs.





TOP THREAT ACTORS

Threat Actor	IOC Reference
UNC2970	https://www.proofpoint.com/us/blog/threat-insight/ta569-socgholish-and-beyond?&web_view=true
TA542	https://github.com/curated-intel/Log4Shell-IOCs
Roayl Ransomeware	https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
YoroTrooper	https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/?&web_view=true
APT32	https://www.rewterz.com/rewterz-news/rewterz-threat-alert-apt32-ocean-lotus-active-iocs-24/

TOP EXPLOITED VULNERABILITIES

Threat	Description	Reference Link
A New Zero day Microsoft Outlook Vulnerability Actively Exploited in the Wild CVE-2023-23397	An Elevation of Privilege (EoP) vulnerability exists in Microsoft Outlook which allow an attacker sends a message to the victim with an extended MAPI property that contains a UNC path.	Critical Privilege Elevation Vulnerability Patched by Microsoft | Cyble Research & Intelligence Labs
Ivanti Avalanche Remote Control Server RCServlet Authentication Bypass Vulnerability CVE-2022-44574	Vulnerability allows remote attackers to bypass authentication on affected installations of Ivanti Avalanche. Authentication is not required to exploit this vulnerability.	ZDI-23-228 | Zero Day Initiative
Siemens Tecnomatix Plant Simulation SPP File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability CVE-2023-27398	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Siemens Tecnomatix Plant Simulation.	ZDI-23-325 | Zero Day Initiative
Adobe Dimension USD File Parsing Memory Corruption Remote Code Execution Vulnerability CVE-2023-25901	Vulnerability allows remote attackers to execute arbitrary code on affected installations of Adobe Dimension. User interaction is equireed to exploit this vulnerability	ZDI-23-289 | Zero Day Initiative
TP-Link Archer AX21 tdpServer Logging Stack-based Buffer Overflow Remote Code Execution Vulnerability CVE-2023-27332	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Archer AX21 routers. Authentication is not required to exploit this vulnerability.	ZDI-23-245 | Zero Day Initiative
Microsoft Windows win32kfull Bitmap Use-After-Free Local Privilege Escalation Vulnerability CVE-2023-24861	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-23-243 | Zero Day Initiative
ManageEngine ServiceDesk Plus MSP generateSQLReport Improper Input Validation Privilege Escalation Vulnerability CVE-2023-26600	Vulnerability allows remote attackers to escalate privileges on affected installations of ManageEngine ServiceDesk Plus MSP. The specific flaw exists within the generateSQLReport function.	ZDI-23-229 | Zero Day Initiative
Trend Micro TXOne StellarOne Improper Access Control Privilege Escalation Vulnerability CVE-2023-25069	Vulnerability allows remote attackers to escalate privileges on affected installations of Trend Micro TXOne StellarOne. The specific flaw exists within the Account endpoint.	ZDI-23-231 | Zero Day Initiative
NETGEAR CAX30S SSO Command Injection Remote Code Execution Vulnerability CVE-2022-43654	Vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR CAX30S routers. The specific flaw exists within the handling of the token parameter provided to the sso.php endpoint.	ZDI-23-214 | Zero Day Initiative

Security Bulletin

1. Nexus, an android malware, is targeting customers of 450 financial institutions worldwide

- Nexus is an Android trojan is targeting customers of 450 banks and cryptocurrency services worldwide which has multiple features for hijacking online accounts and potentially siphoning funds out of them.
- Malware authors of "Nexus" Android Trojan have also made the malware available to other threat actors via a newly announced malware-as-a-service (MaaS) program.
- Nexus contains several features for enabling account takeover. It consists of function for performing overlay attacks and logging keystrokes to steal user credentials, a feature that quietly deletes received SMS two-factor authentication messages and a function for stopping or activating the module for stealing Google Authenticator 2FA codes.
- After compromising a device, when a customer of a target banking or cryptocurrency app attempts to access their account, Nexus serves up a page that looks and functions exactly like the login page for the real app. The malware then uses its keylogging feature to grab the victim's credentials as entered in the login page.
- As per a recent analysis, it has been found that roughly 200,000 new banking trojans surfaced in 2022, representing a 100% increase over 2021.

2. Cyber Espionage on the rise globally targeting multiple countries worldwide

- The Dark Pink APT group targets government entities in ASEAN countries using multiple KamiKaKaBots.
- Russia and Belarus aligned APT group '**Winter Vivern**' is targeting government and private entities in various countries. Their past activity shows campaigns targeting Polish government agencies, the Ukraine Ministry of Foreign Affairs, the Italy Ministry of Foreign Affairs, and individuals within the Indian government as well as private businesses, including telecommunications organizations that support Ukraine in the ongoing war.
- **Sharp Panda**, a Chinese cyber espionage group targeting government entities in Southeast Asia especially countries like Vietnam, Thailand and Indonesia which has similar territorial claims or strategic infrastructure projects using the Soul malware framework.
- **Earth Kitsune** APT group targeting selective individuals in China and Japan showing an interest in North Korea using a previously unknown backdoor WhiskerSpy while another APT group name **Earth Yako** has been targeting entities in Japan by abusing legitimate services such as Dropbox, GitHub, and Protonmail.
- Chinese state-sponsored hacking group, **Mustang Panda** targeting entities in Europe and Asia Pacific via an ongoing social engineering campaign and a custom backdoor named MQsTTang. While another Chinese state-sponsored group, **DEV-0147** has been targeting entities in South America using typical espionage and exfiltration tools like ShadowPad.
- **WIP26** abuse cloud infrastructure of Telecom companies in Middle east in a cyber espionage campaign while **APT41/Winnti**, another cyber espionage group is targeting companies in materials technology sector in Asia in order to steal intellectual property.

3. ChatGPT is a growing risk for businesses and a new cyber threat

- The rise of ChatGPT and its widespread use due to its simple question and answer interface can be a great risk for businesses. One issue could be the ingestion of sensitive business data into ChatGPT which puts organizations at risk.
- Security experts fear that if one inputs sensitive business information like quarterly reports, materials for an internal presentation, sales numbers, or the like — and asks ChatGPT to write text around it, then anyone could gain information on that company simply by asking ChatGPT about it later.
- ChatGPT's latest version GPT-4 is intelligent enough to pass the bar exams, write thousands of words of informational text and it has already started being tested to write malicious code like information stealers by malware authors.
- ChatGPT as a cyberattack tool is still not in its prime and as useful, but it does pose a long-term threat while its use as a task automater should be done with caution by businesses due to the risk of sensitive data leak.
- Developers of ChatGPT and other similar tools have put in filters and controls — and are constantly improving them — to try to limit misuse of their technologies. Another good way of securing these tools would be to

implement authentication and authorization requirements in order to use these AI engines with something similar to what online financial institutions and payment systems currently use.

4. Threat Actors exploring and deploying new attack techniques: Use of QR Codes and Google Translate

- Hackers are experimenting and devising new attack techniques to circumvent new defensive security challenges and are abusing QR codes, Google Translate and other tools.
- QR Code is being used increasingly in phishing campaigns by attackers. Attackers trick users into scanning QR codes on their PCs using their mobile devices – potentially to take advantage of weaker phishing protection and detection on such devices.
- Malicious pdf attachments have risen by 38%, which contains embedded images that link to encrypted malicious ZIP files, bypassing web gateway scanners. The PDF instructions contain a password that the user is tricked into entering to unpack a ZIP file, deploying QakBot or IcedID malware to gain unauthorized access to systems, which is eventually used to deploy ransomware.
- Archive files like ZIP, RAR and IMG are being used by 42% of the malware as threat actors switch to scripts to run their payloads.
- BEC threat actors are using Google Translate to impersonate executives by properly researching their responsibilities and relationship with the Top management in the organization.

5. Okta accidently exposing user password in audit logs

- Okta, the identity access and management (IAM) provider saves user password to audit logs (in clear text) if a user accidentally types them in the “username” field when logging in.
- In recent research, this vulnerability has been uncovered in Okta that allows adversaries to read cleartext user passwords and gain access into a corporate environment as a post exploitation attack method.
- This vulnerability exists because Okta audit logs store detailed information about user activity, including usernames, IP addresses, and login timestamps. The logs also provide information into successful and unsuccessful login attempts and if these attempts were performed via Web browser or mobile app.
- Even though these logs are only accessible to platform administrators in Okta – there can be a number of other ways by which attackers could gain access to these logs like via a SIEM user with read-only privileges or via third party services which have read-only access to Okta configurations – hence providing these users with access to the Okta user passwords, including Okta admins.
- The risks of this feature from Okta can be mitigated by enabling MFA, user awareness and training to avoid entering passwords in Username field, logging and monitoring of suspicious login activities as well as enforcing password rotation within organizations.

REFERENCE LINKS

- https://www.ndtv.com/india-news/in-massive-data-breach-details-of-16-8-crore-citizens-leaked-7-arrested-3886885
- https://cybernews.com/security/lionsgate-data-leak/
- https://www.helpnetsecurity.com/2023/03/20/mid-sized-businesses-cybersecurity-challenges/?web_view=true
- https://www.infosecurity-magazine.com/news/bec-volumes-double-on-phishing/?&web_view=true
- https://www.helpnetsecurity.com/2023/02/22/cve-2023-20858/
- https://www.darkreading.com/application-security/microsoft-outlook-vulnerability-2023-it-bug
- https://www.darkreading.com/attacks-breaches/controlling-third-party-data-risk-should-be-a-top-cybersecurity-priority-
- https://www.darkreading.com/attacks-breaches/attackers-probing-zero-day-vulns-edge-infrastructure
- https://www.darkreading.com/mobile/new-android-malware-targets-customers-of-450-financial-institutions-worldwide
- https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
- https://www.darkreading.com/mobile/new-android-malware-targets-customers-of-450-financial-institutions-worldwide
- https://blog.eclecticiq.com/dark-pink-apt-group-strikes-government-entities-in-south-asian-countries
- https://www.sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/?&web_view=true
- https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/
- https://cyware.com/news/newly-identified-earth-yako-apt-observed-targeting-japanese-entities-2b609c3f
- https://cyware.com/news/earth-kitsun-return-to-target-selected-entities-in-china-and-japan-dfb0538f
- https://cyware.com/news/chinese-espionage-group-dev-0147-targets-diplomatic-entities-in-south-america-085a1297
- https://cyware.com/news/chinese-hackers-target-asian-and-european-entities-with-mqsttang-db2facc8
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackfly-espionage-materials?web_view=true
- https://www.darkreading.com/attacks-breaches/attackers-are-already-exploiting-chatgpt-to-write-malicious-code
- https://www.csoonline.com/article/3691115/sharing-sensitive-business-data-with-chatgpt-could-be-risky.html#tk.rss_news
- https://www.helpnetsecurity.com/2023/03/21/qr-scan-scams/?web_view=true
- https://www.csoonline.com/article/3688429/bec-groups-are-using-google-translate-to-target-high-value-victims.html?&web_view=true
- Tick APT Targeted High-Value Customers of East Asian Data-Loss Prevention Company (thehackernews.com)
- Talos uncovers espionage campaigns targeting CIS countries, embassies and EU health care agency (talosintelligence.com)

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**.

55 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com