Hacking Groups
Targeting the Aerospace Industry

by
Buğra YELER

✉ bugrayeler5@gmail.com

Abstract

In recent days, due to incrementing on the popularization of cyber security attack, the importance of data security has increased. In that report, information about the hacking groups which targeting the aerospace industry. There is information about all of known names in industry, located country, first seen operation, description, targeted industries and countries, used tools, used techniques and operation performed for each group.

Contents

.

Name	Lazarus Group -> (Kaspersky)
Other Names	Hidden Cobra -> (U.S. Government) Zinc -> (Microsoft & Facebook) Nickel Academy -> (Secureworks Counter Threat Unit) Labyrinth Chollima -> (CrowdStrike) Whois Hacking Team -> (McAfee) Group 77 -> (Talos Group) Hastati Group -> (Dell Secure Works)
Country	🇰🇵 North Korea
First seen	2009
Description	Lazarus group which is a threat group that has been attributed to the North Korean government, has been active for nearly 12 years. We heard Lazarus Group name first in the reported that responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Based on analysis of the extensive malware set and details found in public reporting from attacks, the Lazarus Group appears to have resources that allow for development of custom malware tools for extensive, coordinated and, targeted attacks, including long periods of reconnaissance. Malware used by Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.
Targets	**Sectors:** Aerospace, Engineering, Financial, Government, Media, Shipping and Logistics, Technology and BitCoin exchanges. **Countries:** Australia, Bangladesh, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam and Worldwide (WannaCry).
Tools used	**AppleJeus** [(https://attack.mitre.org/software/S0584/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=AppleJeus)]

	AuditCred [(https://attack.mitre.org/software/S0347/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=AuditCred)] **BADCALL** [(https://attack.mitre.org/software/S0245/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=BADCALL)] **Bankshot** [(https://attack.mitre.org/software/S0239/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Bankshot)] **BLINDINGCAN** [(https://attack.mitre.org/software/S0520/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=BLINDINGCAN)] **Dacls** [(https://attack.mitre.org/software/S0497/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Dacls%20RAT)] **Dtrack** [(https://attack.mitre.org/software/S0567/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Dtrack)] **FALLCHILL** [(https://attack.mitre.org/software/S0181/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=FALLCHILL)] **HARDRAIN** [(https://attack.mitre.org/software/S0246/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=HARDRAIN)] **HOPLIGHT** [(https://attack.mitre.org/software/S0376/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=HOPLIGHT)] **KEYMARBLE** [(https://attack.mitre.org/software/S0271/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=KEYMARBLE)] **Mimikatz** [(https://attack.mitre.org/software/S0002/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Mimikatz)] **Proxysvc** [(https://attack.mitre.org/software/S0238/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Proxysvc)] **RATANKBA** [(https://attack.mitre.org/software/S0241/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Ratankba)] **RawDisk** [(https://attack.mitre.org/software/S0364/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=RawDisk)] **TAINTEDSCRIBE** [(https://attack.mitre.org/software/S0586/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=TAINTEDSCRIBE)] **TYPEFRAME** [(https://attack.mitre.org/software/S0263/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=TYPEFRAME)]

	Volgmer [(https://attack.mitre.org/software/S0180/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Volgmer)] **WannaCry** [(https://attack.mitre.org/software/S0366/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=WannaCry)]	
Techniques used	**Name**	**Use**
	Access Token Manipulation: Create Process with Token	Lazarus Group keylogger KiloAlfa obtains user tokens from interactive sessions to execute itself with API call CreateProcessAsUserA under that user's context.
	Account Manipulation	Lazarus Group malware WhiskeyDelta-Two contains a function that attempts to rename the administrator’s account.
	Acquire Infrastructure: Domains	Lazarus Group has acquired infrastructure related to their campaigns to act as distribution points and C2 channels.
	Acquire Infrastructure: Web Services	Lazarus Group has hosted malicious downloads on Github.
	Application Layer Protocol: Web Protocols	Lazarus Group malware has conducted C2 over HTTP and HTTPS.
	Application Window Discovery	Lazarus Group malware IndiaIndia obtains and sends to its C2 server the title of the window for each running process. The KilaAlfa keylogger also reports the title of the window in the foreground.
	Archive Collected Data	Lazarus Group malware RomeoDelta archives specified directories in .zip format, encrypts the .zip file, and uploads it to its C2 server.
	Archive via Library	Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is compressed with Zlib, encrypted, and uploaded to a C2 server.

	Archive via Custom Method	A Lazarus Group malware sample encrypts data using a simple byte based XOR operation prior to exfiltration.
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Lazarus Group malware attempts to maintain persistence by saving itself in the Start menu folder or by adding a Registry Run key.
	Boot or Logon Autostart Execution: Security Support Provider	Lazarus Group has rebooted victim machines to establish persistence by installing a SSP DLL.
	Boot or Logon Autostart Execution: Shortcut Modification	A Lazarus Group malware sample adds persistence on the system by creating a shortcut in the user's Startup folder.
	Brute Force: Password Spraying	Lazarus Group malware attempts to connect to Windows shares for lateral movement by using a generated list of usernames, which center around permutations of the username Administrator, and weak passwords.
	Command and Scripting Interpreter: PowerShell	Lazarus Group has used Powershell to download malicious payloads.
	Command and Scripting Interpreter: Windows Command Shell	Lazarus Group malware uses cmd.exe to execute commands on victims. A Destover-like variant used by Lazarus Group uses a batch file mechanism to delete its binaries from the system.
	Command and Scripting Interpreter: Visual Basic	Lazarus Group has used VBScript to gather information about a victim machine.
	Create or Modify System Process: Windows Service	Several Lazarus Group malware families install themselves as new services on victims.
	Data Destruction	Lazarus Group has used a custom secure delete function to overwrite file contents with data from heap memory.

	Data Encoding: Standard Encoding	A Lazarus Group malware sample encodes data with base64.
	Data from Local System	Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is uploaded to one of its 10 C2 servers. Lazarus Group malware RomeoDelta copies specified directories from the victim's machine, then archives and encrypts the directories before uploading to its C2 server. Lazarus Group has used wevtutil to export Window security event logs.
	Data Obfuscation: Protocol Impersonation	Lazarus Group malware also uses a unique form of communication encryption known as FakeTLS that mimics TLS but uses a different encryption method, evading SSL man-in-the-middle decryption attacks.
	Data Staged: Local Data Staging	Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is saved in the %TEMP% directory, then compressed, encrypted, and uploaded to a C2 server.
	Defacement: Internal Defacement	Lazarus Group replaced the background wallpaper of systems with a threatening image after rendering the system unbootable with a Disk Structure Wipe
	Develop Capabilities: Malware	Lazarus Group has developed several custom malware for use in operations.
	Disk Wipe: Disk Content Wipe	Lazarus Group has used malware like WhiskeyAlfa to overwrite the first 64MB of every drive with a mix of static and random buffers. A similar process is then used to wipe content in logical drives and, finally, attempt to wipe every byte of every sector on every drive. WhiskeyBravo can be used to overwrite the first 4.9MB of physical drives. WhiskeyDelta can overwrite the first 132MB or 1.5MB of each drive with random data from heap memory.

	Disk Wipe: Disk Structure Wipe	Lazarus Group malware SHARPKNOT overwrites and deletes the Master Boot Record (MBR) on the victim's machine and has possessed MBR wiper malware since at least 2009.
	Drive-by Compromise	Lazarus Group delivered RATANKBA to victims via a compromised legitimate website.
	Encrypted Channel: Symmetric Cryptography	Several Lazarus Group malware families encrypt C2 traffic using custom code that uses XOR with an ADD operation and XOR with a SUB operation. Another Lazarus Group malware sample XORs C2 traffic. Other Lazarus Group malware uses Caracachs encryption to encrypt C2 payloads.
	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Lazarus Group malware SierraBravo-Two generates an email message via SMTP containing information about newly infected victims.
	Exfiltration Over C2 Channel	Lazarus Group malware IndiaIndia saves information gathered about the victim to a file that is uploaded to one of its 10 C2 servers. Another Lazarus Group malware sample also performs exfiltration over the C2 channel.
	Exploitation for Client Execution	Lazarus Group has exploited Adobe Flash vulnerability CVE-2018-4878 for execution.
	Fallback Channels	Lazarus Group malware SierraAlfa sends data to one of the hard-coded C2 servers chosen at random, and if the transmission fails, chooses a new C2 server to attempt the transmission again.
	File and Directory Discovery	Several Lazarus Group malware samples use a common function to identify target files by their extension. Lazarus Group malware families can also enumerate files and directories, including a Destover-like variant that lists files and gathers information for all drives.

	Hide Artifacts: Hidden Files and Directories	Lazarus Group has used a VBA Macro to set its file attributes to System and Hidden and has named files with a dot prefix to hide them from the Finder application.
	Impair Defenses: Disable or Modify Tools	Lazarus Group malware TangoDelta attempts to terminate various processes associated with McAfee. Additionally, Lazarus Group malware SHARPKNOT disables the Microsoft Windows System Event Notification and Alerter services. During a 2019 intrusion, Lazarus Group disabled Windows Defender and Credential Guard as some of their first actions on host.
	Impair Defenses: Disable or Modify System Firewall	Various Lazarus Group malware modifies the Windows firewall to allow incoming connections or disable it entirely using netsh.
	Indicator Removal on Host: File Deletion	Lazarus Group malware deletes files in various ways, including "suicide scripts" to delete malware binaries from the victim. Lazarus Group also uses secure file deletion to delete files from the victim.
	Indicator Removal on Host: Timestomp	Several Lazarus Group malware families use timestomping, including modifying the last write timestamp of a specified Registry key to a random date, as well as copying the timestamp for legitimate .exe files (such as calc.exe or mspaint.exe) to its dropped files.
	Ingress Tool Transfer	Several Lazarus Group malware families are capable of downloading and executing binaries from its C2 server.
	Input Capture: Keylogging	Lazarus Group malware KiloAlfa contains keylogging functionality.
	Masquerading: Masquerade Task or Service	A Lazarus Group custom backdoor implant included a custom PE loader named "Security Package" that was added into the lsass.exe process via registry key.

	Masquerading: Match Legitimate Name or Location	Lazarus Group has renamed the TAINTEDSCRIBE main executable to disguise itself as Microsoft's narrator.
	Modify Registry	Lazarus Group has modified registry keys using the reg windows utility for its custom backdoor implants.
	Non-Standard Port	Some Lazarus Group malware uses a list of ordered port numbers to choose a port for C2 traffic, creating port-protocol mismatches.
	Obfuscated Files or Information	Lazarus Group malware uses multiple types of encryption and encoding in its malware files, including AES, Caracachs, RC4, basic XOR with constant 0xA7, and other techniques.
	Software Packing	Lazarus Group has used Themida to pack at least two separate backdoor implants.
	Obtain Capabilities: Digital Certificates	Lazarus Group has obtained SSL certificates for their C2 domains.
	OS Credential Dumping: LSASS Memory	Lazarus Group leveraged Mimikatz to extract Windows Credentials of currently logged-in users and steals passwords stored in browsers. Lazarus Group has also used a custom version Mimikatz to capture credentials.
	Phishing: Spearphishing Attachment	Lazarus Group has targeted victims with spearphishing emails containing malicious Microsoft Word documents.
	Phishing: Spearphishing via Service	Lazarus Group has used fake job advertisements sent via LinkedIn to spearphish victims.
	Pre-OS Boot: Bootkit	Lazarus Group malware WhiskeyAlfa-Three modifies sector 0 of the Master Boot Record (MBR) to ensure that the malware will persist even if a victim machine shuts down.

	Process Discovery	Several Lazarus Group malware families gather a list of running processes on a victim system and send it to their C2 server. A Destover-like variant used by Lazarus Group also gathers process times.
	Process Injection: Dynamic-link Library Injection	A Lazarus Group malware sample performs reflective DLL injection.
	Proxy: External Proxy	Lazarus Group uses multiple proxies to obfuscate network traffic from victims.
	Query Registry	Lazarus Group malware IndiaIndia checks Registry keys within HKCU and HKLM to determine if certain applications are present, including SecureCRT, Terminal Services, RealVNC, TightVNC, UltraVNC, Radmin, mRemote, TeamViewer, FileZilla, pcAnyware, and Remote Desktop. Another Lazarus Group malware sample checks for the presence of the following Registry key:HKEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt.
	Remote Services: Remote Desktop Protocol	Lazarus Group malware SierraCharlie uses RDP for propagation.
	Remote Services: SMB/Windows Admin Shares	Lazarus Group malware SierraAlfa accesses the ADMIN$ share via SMB to conduct lateral movement.
	Resource Hijacking	Lazarus Group has subset groups like Bluenoroff who have used cryptocurrency mining software on victim machines.
	Service Stop	Lazarus Group has stopped the MSExchangeIS service to render Exchange contents inaccessible to users.
	Signed Binary Proxy Execution: Compiled HTML File	Lazarus Group has used CHM files to move concealed payloads.

	Signed Binary Proxy Execution: Mshta	Lazarus Group has used mshta.exe to run malicious scripts and download programs.
	System Information Discovery	Several Lazarus Group malware families collect information on the type and version of the victim OS, as well as the victim computer name and CPU information. A Destover-like variant used by Lazarus Group also collects disk space information and sends it to its C2 server.
	System Network Configuration Discovery	Lazarus Group malware IndiaIndia obtains and sends to its C2 server information about the first network interface card's configuration, including IP address, gateways, subnet mask, DHCP information, and whether WINS is available.
	System Owner/User Discovery	Various Lazarus Group malware enumerates logged-on users.
	System Shutdown/Reboot	Lazarus Group has rebooted systems after destroying files and wiping the MBR on infected systems.
	System Time Discovery	A Destover-like implant used by Lazarus Group can obtain the current system time and send it to the C2 server.
	User Execution: Malicious File	Lazarus Group has attempted to get users to launch a malicious Microsoft Word attachment delivered via a spearphishing email.
	Windows Management Instrumentation	Lazarus Group malware SierraAlfa uses the Windows Management Instrumentation Command-line application wmic to start itself on a target system during lateral movement.

Operations performed	**Date**	**Name**	**Target & Method**
	Jul 2009	Operation "Troy"	**Target:** Government, financial and media institutions in South Korea and USA. **Method:** DdoS attacks.

	Mar 2011	Attack on South Korean banks and media	**Target:** South Korean organizations. **Method:** DdoS attacks and destruction of infected machines.
	Mar 2013	Operation “Ten Days of Rain” / ”DarkSeoul”	**Target:** Three broadcasting stations and a bank in South Korea. **Method:** Infecting with viruses, stealing and wiping information.
	Nov 2014	Operation “Blockbuster”: Breach of Sony Pictures Entertainment	**Target:** Sony Pictures Entertainment (released the “Interview” movie, ridiculing the North Korean leader). **Method:** Infecting with malware, stealing and wiping data of the company’s employees, correspondence, copies of unreleased films.
	Apr 2018	Operation “GhostSecret”	**Target:** The impacted organizations are in industries such as telecommunications, health, finance, critical infrastructure, and entertainment. **Method:** Spear-phishing with Destover-like implant.
	Aug 2018	Operation “AppleJeus”	**Target:** Cryptocurrency exchange. **Method:** Fake installer and macOS malware.
	Oct 2018	Operation “Sharpshooter”	**Target:** 87 organizations in many different sectors (majority Government and Defense) across the globe, predominantly in the United States. **Method:** Rising Sun implant to gather intelligence.
	Sep 2019	Operation “In(ter)caption”	**Target:** Aerospace and military companies in Europe and the Middle East **Method: -**

Name	Reaper -> (FireEye)
Other Names	APT 37 -> (Mandiant) ScarCruft -> (Kaspersky) Group 123 -> (Talos) Ricochet Chollima -> (CrowdStrike) Red Eyes -> (AhnLab)
Country	🇰🇵 North Korea
First seen	2012
Description	Reaper which has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East, has been active for nearly 10 years. Reaper group is rumored to have a wide range of Infiltration capabilities, like planting custom-coded malware on target's devices, capable of eavesdropping, recording audio logs via the infected system and completely wiping the drive to leave no footprint. Their malwares are primarily focused on stealing information and are set up to automatically exfiltrate data of interest from the infected user's system. One of the identified malware by the Reaper is called 'DogCall', which allows them to, log keystrokes, access cloud storage services like Dropbox and take screenshots. In March and April of 2017, it was used to target South Korean government as well as military organizations.
Targets	**Sectors:** Various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare. **Countries:** Primarily South Korea, though also Japan, Vietnam and the Middle East.
Tools used	**CORALDECK** [(https://attack.mitre.org/software/S0212/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=CORALDECK)] **DOGCALL** [(https://attack.mitre.org/software/S0213/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=DOGCALL)] **Final1stspy** [(https://attack.mitre.org/software/S0355/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Final1stSpy)] **HAPPYWORK** [(https://attack.mitre.org/software/S0214/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=HAPPYWORK)]

	KARAE [(https://attack.mitre.org/software/S0215/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=KARAE)] **NavRAT** [(https://attack.mitre.org/software/S0247/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=NavRAT)] **POORAIM** [(https://attack.mitre.org/software/S0216/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=POORAIM)] **ROKRAT** [(https://attack.mitre.org/software/S0240/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=RokRAT)] **SHUTTERSPEED** [(https://attack.mitre.org/software/S0217/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=SHUTTERSPEED)] **SLOWDRIFT** [(https://attack.mitre.org/software/S0218/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=SLOWDRIFT)] **WINERACK** [(https://attack.mitre.org/software/S0219/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=WINERACK)	
Techniques used	**Name**	**Use**
	Abuse Elevation Control Mechanism: Bypass User Account Control	Reaper has a function in the initial dropper to bypass Windows UAC in order to execute the next payload with higher privileges.
	Application Layer Protocol: Web Protocols	Reaper uses HTTPS to conceal C2 communications.
	Audio Capture	Reaper has used an audio capturing utility known as SOUNDWAVE that captures microphone input.
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Reaper's has added persistence via the Registry key HKCU\Software\Microsoft\CurrentVersion\Run\.
	Command and Scripting Interpreter: Windows Command Shell	Reaper has used the command-line interface.

	Command and Scripting Interpreter: Visual Basic	Reaper executes shellcode and a VBA script to decode Base64 strings.
	Credentials from Password Stores: Credentials from Web Browsers	Reaper has used a credential stealer known as ZUMKONG that can harvest usernames and passwords stored in browsers.
	Data from Local System	Reaper has collected data from victims' local systems.
	Disk Wipe: Disk Structure Wipe	Reaper has access to destructive malware that is capable of overwriting a machine's Master Boot Record (MBR).
	Drive-by Compromise	Reaper has used strategic web compromises, particularly of South Korean websites, to distribute malware. The group has also used torrent file-sharing sites to more indiscriminately disseminate malware to victims. As part of their compromises, the group has used a Javascript based profiler called RICECURRY to profile a victim's web browser and deliver malicious code accordingly.
	Exploitation for Client Execution	Reaper has used Flash Player (CVE-2016-4117, CVE-2018-4878) and Word (CVE-2017-0199) exploits for execution.
	Ingress Tool Transfer	Reaper has downloaded second stage malware from compromised websites.
	Inter-Process Communication: Dynamic Data Exchange	Reaper has used Windows DDE for execution of commands and a malicious VBS.
	Masquerading: Invalid Code Signature	Reaper has signed its malware with an invalid digital certificates listed as "Tencent Technology (Shenzhen) Company Limited".

	Native API	Reaper leverages the Windows API calls: VirtualAlloc(), WriteProcessMemory(), and CreateRemoteThread() for process injection.
	Obfuscated Files or Information	Reaper obfuscates strings and payloads.
	Steganography	Reaper uses steganography to send images to users that are embedded with shellcode.
	Peripheral Device Discovery	Reaper has a Bluetooth device harvester, which uses Windows Bluetooth APIs to find information on connected Bluetooth devices.
	Phishing: Spearphishing Attachment	Reaper delivers malware using spearphishing emails with malicious HWP attachments.
	Process Discovery	Reaper Freenki malware lists running processes using the Microsoft Windows API.
	Process Injection	Reaper injects its malware variant, ROKRAT, into the cmd.exe process.
	System Information Discovery	Reaper collects the computer name, the BIOS model, and execution path.
	System Owner/User Discovery	Reaper identifies the victim username.
	System Shutdown/Reboot	Reaper has used malware that will issue the command shutdown /r /t 1 to reboot a system after wiping its MBR.
	User Execution: Malicious File	Reaper has sent spearphishing attachments attempting to get a user to open them.

	Web Service: Bidirectional Communication		Reaper leverages social networking sites and cloud platforms (AOL, Twitter, Yandex, Mediafire, pCloud, Dropbox, and Box) for C2.
Operations performed	**Date**	**Name**	**Target & Method**
	Mar 2016	Operation “Daybreak”	**Target:** High profile victims. **Method:** Previously unknown (0-day) Adobe Flash Player exploit. It is also possible that the group deployed another zero day exploit, CVE-2016-0147, which was patched in April.
	Aug 2016	Operation “Golden Time”	**Target:** South Korean users. **Method:** Spear-phishing emails combined with malicious HWP documents created using Hancom Hangul Office Suite.
	Nov 2016	Operation “Evil New Year”	**Target:** South Korean users. **Method:** Spear-phishing emails combined with malicious HWP documents created using Hancom Hangul Office Suite.
	Mar 2017	Operation “Are You Happy?”	**Target:** South Korean users. **Method:** Not only to gain access to the remote infected systems but to also wipe the first sectors of the device.
	May 2017	Operation “FreeMilk”	**Target:** Several non-Korean financial institutions. **Method:** A malicious Microsoft Office document, a deviation from their normal use of Hancom documents.
	Nov 2017	Operation “North Korean Human Right”	**Target:** South Korean users. **Method:** Spear-phishing emails combined with malicious HWP documents created using Hancom Hangul Office Suite.
	Jan 2018	Operation “Evil New Year 2018”	**Target:** South Korean users. **Method:** Spear-phishing emails combined with malicious HWP documents created using Hancom Hangul Office Suite.

<table>
<tr><td><b>Name</b></td><td>Cutting Kitten -> <i>(CrowdStrike)</i></td></tr>
<tr><td><b>Other Names</b></td><td>TG-2889 -> (SecureWorks)
Cleaver -> (Crowdstrike)</td></tr>
<tr><td><b>Country</b></td><td>🇮🇷 Iran</td></tr>
<tr><td><b>First seen</b></td><td>2012</td></tr>
<tr><td><b>Description</b></td><td>Cutting Kitten is a threat group that estimated Cleaver is linked to Threat Group 2889, has been attributed to Iranian actors and is responsible for activity tracked as Operation Cleaver.
A research of the Cleaver group by Dell SecureWorks Counter Threat Unit (CTU) researchers uncovered a network of fake LinkedIn profiles that target potential victims through social engineering.</td></tr>
<tr><td><b>Targets</b></td><td><b>Sectors:</b> Aerospace, Aviation, Chemical, Defense, Education, Energy, Financial, Government, Healthcare, Oil and gas, Technology, Telecommunications, Transportation, Utilities and (banks: Bank of America, US Bancorp, Fifth Third Bank, Citigroup, PNC, BB&T, Wells Fargo, Capital One and HSBC).
<b>Countries:</b> Canada, China, France, Germany, India, Israel, Kuwait, Mexico, Netherlands, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, UAE, UK, USA.</td></tr>
<tr><td><b>Tools used</b></td><td><b>Mimikatz</b> [(https://attack.mitre.org/software/S0002/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Mimikatz)]
<b>Net Crawler</b> [(https://attack.mitre.org/software/S0056/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Net%20Crawler)]
<b>TinyZBot</b> [(https://attack.mitre.org/software/S0004/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=TinyZBot)]</td></tr>
<tr><td><b>Techniques used</b></td><td><table><tr><th>Name</th><th>Use</th></tr><tr><td>Develop Capabilities: Malware</td><td>Cutting Kitten has created customized tools and payloads for functions including ARP poisoning, encryption, credential dumping, ASP.NET shells, web backdoors, process enumeration, WMI querying, HTTP and SMB communications, network interface sniffing, and keystroke logging.</td></tr></table></td></tr>
</table>

	Establish Accounts: Social Media Accounts		Cutting Kitten has created fake LinkedIn profiles that included profile photos, details, and connections.
	Man-in-the-Middle: ARP Cache Poisoning		Cutting Kitten has used custom tools to facilitate ARP cache poisoning.
	OS Credential Dumping: LSASS Memory		Cutting Kitten has been known to dump credentials using Mimikatz and Windows Credential Editor.
Operations performed	**Date**	**Name**	**Target & Method**
	2012	Operation "Cleaver"	**Target:** Military, oil and gas, energy and utilities, transportation, airlines, airports, hospitals, telecommunications, technology, education, aerospace, Defense Industrial Base (DIB), chemical companies, and governments. **Method:** Used a set of tools that can spy on and potentially shut down critical control systems and computer networks, aiming.
	2013	Attack on the Bowman Avenue Dam	**Target:** A small dam less than 20 miles from New York City. **Method:** -
	2015	Network of Fake LinkedIn Profiles	**Target:** Middle Eastern and North African mobile telephony suppliers, Worker at Middle Eastern governments and for defense organizations based in the Middle East and South Asia. **Method:** Used a network of fake LinkedIn profiles, targeted potential victims through social engineering.

Name	Chafer -> (Symantec)
Other Names	APT 39 -> (Mandiant) Remix Kitten -> (CrowdStrike) Cobalt Hickman -> (SecureWorks) TA454 -> (Proofpoint) ITG07 -> (IBM)
Country	Iran
First seen	2014
Description	Chafer which is known as APT39, is one of several names for cyberespionage activity conducted by the Iranian Ministry of Intelligence and Security (MOIS) through the front company Rana Intelligence Computing since at least 2014. APT39 has primarily targeted the travel, hospitality, academic, and telecommunications industries in Iran and across Asia, Africa, Europe, and North America to track individuals and entities considered to be a threat by the MOIS.
Targets	**Sectors:** Aerospace, Aviation, Engineering, Government, High-Tech, IT, Shipping and Logistics, Telecommunications, Transportation. **Countries:** Israel, Jordan, Kuwait, Saudi Arabia, Spain, Turkey, UAE, USA and Middle East.
Tools used	**ASPXSpy** [(https://attack.mitre.org/software/S0073/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=ASPXSpy)] **MechaFlounder** [(https://attack.mitre.org/software/S0459/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=MechaFlounder)] **Mimikatz** [(https://attack.mitre.org/software/S0002/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Mimikatz)] **NBTscan** [(https://attack.mitre.org/software/S0590/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=nbtscan)] **Pwdump** [(https://attack.mitre.org/software/S0006/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=pwdump)] **Remexi** [(https://attack.mitre.org/software/S0375/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Remexi)]

	Windows Credential Editor [(https://attack.mitre.org/software/S0005/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Windows%20Credentials%20Editor)]	
Techniques used	**Name**	**Use**
	Application Layer Protocol: Web Protocols	Chafer has used HTTP in communications with C2.
	Application Layer Protocol: DNS	Chafer has used remote access tools that leverage DNS in communications with C2.
	Archive Collected Data: Archive via Utility	Chafer has used WinRAR and 7-Zip to compress an archive stolen data.
	BITS Jobs	Chafer has used the BITS protocol to exfiltrate stolen data from a compromised host.
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Chafer has maintained persistence using the startup folder.
	Boot or Logon Autostart Execution: Shortcut Modification	Chafer has modified LNK shortcuts.
	Brute Force	Chafer has used Ncrack to reveal credentials.
	Clipboard Data	Chafer has used tools capable of stealing contents of the clipboard.
	Command and Scripting Interpreter	Chafer has utilized AutoIt and custom scripts to perform internal reconnaissance.
	PowerShell	Chafer has used PowerShell to execute malicious code.

	Visual Basic	Chafer has utilized malicious VBS scripts in malware.
	Python	Chafer has used a command line utility and a network scanner written in python.
	Create Account: Local Account	Chafer has created accounts on multiple compromised hosts to perform actions within the network.
	Credentials from Password Stores	Chafer has used the Smartftp Password Decryptor tool to decrypt FTP passwords.
	Data from Local System	Chafer has used various tools to steal files from the compromised host.
	Data Staged: Local Data Staging	Chafer has utilized tools to aggregate data prior to exfiltration.
	Deobfuscate/Decode Files or Information	Chafer has used malware to decrypt encrypted CAB files.
	Event Triggered Execution: AppInit DLLs	Chafer has used malware to set LoadAppInit_DLLs in the Registry key SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows in order to establish persistence.
	Exfiltration Over C2 Channel	Chafer has exfiltrated stolen victim data through C2 communications.
	Exploit Public-Facing Application	Chafer has used SQL injection for initial compromise.

	File and Directory Discovery	Chafer has used tools with the ability to search for files on a compromised host.
	Indicator Removal on Host: File Deletion	Chafer has used malware to delete files after they are deployed on a compromised host
	Ingress Tool Transfer	Chafer has downloaded tools to compromised hosts.
	Input Capture	Chafer has utilized tools to capture mouse movements.
	Keylogging	Chafer has used tools for capturing keystrokes.
	Masquerading: Match Legitimate Name or Location	Chafer has used malware disguised as Mozilla Firefox and a tool named mfevtpse.exe to proxy C2 communications, closely mimicking a legitimate McAfee file mfevtps.exe.
	Network Service Scanning	Chafer has used CrackMapExec and a custom port scanner known as BLUETORCH for network scanning.
	Network Share Discovery	Chafer has used the post exploitation tool CrackMapExec to enumerate network shares.
	Obfuscated Files or Information	Chafer has used malware to drop encrypted CAB files.
	Software Packing	Chafer has packed tools with UPX, and has repacked a modified version of Mimikatz to thwart anti-virus detection.

	OS Credential Dumping	Chafer has used different versions of Mimikatz to obtain credentials.
	LSASS Memory	Chafer has used Mimikatz, Windows Credential Editor and ProcDump to dump credentials.
	Phishing: Spearphishing Attachment	Chafer leveraged spearphishing emails with malicious attachments to initially compromise victims.
	Phishing: Spearphishing Link	Chafer leveraged spearphishing emails with malicious links to initially compromise victims.
	Proxy: Internal Proxy	Chafer used custom tools to create SOCK5 and custom protocol proxies between infected hosts.
	Proxy: External Proxy	Chafer has used various tools to proxy C2 communications.
	Query Registry	Chafer has used various strains of malware to query the Registry.
	Remote Services: Remote Desktop Protocol	Chafer has been seen using RDP for lateral movement and persistence, in some cases employing the rdpwinst tool for mangement of multiple sessions.
	Remote Services: SMB/Windows Admin Shares	Chafer has used SMB for lateral movement.
	Remote Services: SSH	Chafer used secure shell (SSH) to move laterally among their targets.

	Remote System Discovery	Chafer has used NBTscan and custom tools to discover remote systems.
	Scheduled Task/Job: Scheduled Task	Chafer has created scheduled tasks for persistence.
	Screen Capture	Chafer has used a screen capture utility to take screenshots on a compromised host.
	Server Software Component: Web Shell	Chafer has installed ANTAK and ASPXSPY web shells.
	Subvert Trust Controls: Code Signing Policy Modification	Chafer has used malware to turn off the RequireSigned feature which ensures only signed DLLs can be run on Windows.
	System Owner/User Discovery	Chafer used Remexi to collect usernames from the system.
	System Services: Service Execution	Chafer has used post-exploitation tools including RemCom and the Non-sucking Service Manager (NSSM) to execute processes.
	User Execution: Malicious Link	Chafer has sent spearphishing emails in an attempt to lure users to click on a malicious link.
	User Execution: Malicious File	Chafer has sent spearphishing emails in an attempt to lure users to click on a malicious attachment.
	Valid Accounts	Chafer has used stolen credentials to compromise Outlook Web Access (OWA).

	Web Service: Bidirectional Communication	Chafer has communicated with C2 through files uploaded to and downloaded from DropBox.

Operations performed	Date	Name	Target & Method
	2017	Chafer	**Target:** Airlines, aircraft services, software and IT services companies serving the air and sea transport sectors, telecoms services, payroll services, engineering consultancies, and document management software at Israel, Jordan, the United Arab Emirates, Saudi Arabia, and Turkey. **Method:** Chafer use seven new tools in its more recent campaigns, in addition to malware it is previously known to have used. Most of the new tools are freely available, off-the-shelf tools, put to a malicious use. These new tools are Remcom, Non-sucking Service Manager (NSSM), A custom screenshot and clipboard capture tool, SMB hacking tools, GNU HTTPTunnel, UltraVNC and NBTScan.
	Feb 2018	Turkish Government Targeting	**Target:** Turkish Government **Method:** Used a Python-based payload. This payload, now known as MechaFlounder was created by Chafer using a combination of actor developed code and code snippets freely available online in development communities. The MechaFlounder Trojan contains enough functionality for the Chafer actors to carry out the necessary activities needed to accomplish their goals, specifically by supporting file upload and download, as well as command execution functionality.
	Autumn 2018	Spying on Iran-based foreign diplomatic entities	**Target:** Foreign diplomatic entities in Iran. **Method:** The main tool used in this campaign is an updated version of the Remexi malware, publicly reported by Symantec back in 2015. The newest module’s compilation timestamp is March 2018. The developers used GCC compiler on Windows in the MinGW environment

	2018	Iranian Chafer APT Targeted Air Transportation and Government in Kuwait and Saudi Arabia	**Target:** Air Transportation and Government in Kuwait and Saudi Arabia. **Method:** The attack were based on several tools, including “living off the land” tools, which makes attribution difficult, as well as different hacking tools and a custom built backdoor.

Name	Magic Hound -> (Palo Alto)
Other Names	APT 35 -> (Mandiant) Cobalt Illusion -> (SecureWorks) Charming Kitten -> (CrowdStrike) TEMP.Beanie -> (FireEye) Timberworm -> (Symantec) Tarh Andishan -> (Cylance) TA453 -> (Proofpoint) Phosphorus -> (Microsoft)
Country	🇮🇷 Iran
First seen	2014
Description	Magic Hound is an Iranian-sponsored threat group that conducts long term, resource-intensive cyber espionage operations, dating back as early as 2014. The group typically targets organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia. Also targets U.S. and Middle Eastern military organizations, as well as other government personnel, via complex social engineering campaigns.
Targets	**Sectors:** Defense, Energy, Financial, Government, Healthcare, IT, Oil and gas, Technology, Telecommunications and that are either based or have business interests in Saudi Arabia, and ClearSky, HBO, civil and human rights activists and journalists. **Countries:** Afghanistan, Canada, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Morocco, Pakistan, Saudi Arabia, Spain, Syria, Turkey, UAE, UK, USA, Venezuela, Yemen.
Tools used	**DownPaper** [(https://attack.mitre.org/software/S0186/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=DownPaper)] **Mimikatz** [(https://attack.mitre.org/software/S0002/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Mimikatz)] **Pupy** [(https://attack.mitre.org/software/S0192/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=PupyRAT)]

Techniques used	**Name**	**Use**
	Account Manipulation: Exchange Email Delegate Permissions	Magic Hound granted compromised email accounts read access to the email boxes of additional targeted accounts. The group then was able to authenticate to the intended victim's OWA (Outlook Web Access) portal and read hundreds of email communications for information on Middle East organizations.
	Application Layer Protocol	Magic Hound malware has used IRC for C2.
	Web Protocols	Magic Hound malware has used HTTP for C2.
	Archive Collected Data: Archive via Utility	Magic Hound has used RAR to stage and compress local folders.
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Magic Hound malware has used Registry Run keys to establish persistence.
	Command and Scripting Interpreter: PowerShell	Magic Hound has used PowerShell for execution and privilege escalation.
	Command and Scripting Interpreter: Windows Command Shell	Magic Hound has used the command-line interface.
	Command and Scripting Interpreter: Visual Basic	Magic Hound malware has used VBS scripts for execution.
	Compromise Accounts: Email Accounts	Magic Hound has compromised personal email accounts through the use of legitimate credentials and gathered additional victim information.

	Email Collection: Local Email Collection	Magic Hound has collected .PST archives.
	Establish Accounts: Email Accounts	Magic Hound has established email accounts using fake personas for spear-phishing operations.
	File and Directory Discovery	Magic Hound malware can list a victim's logical drives and the type, as well the total/free space of the fixed devices. Other malware can list a directory's contents.
	Gather Victim Identity Information: Credentials	Magic Hound gathered credentials from two victims that they then attempted to validate across 75 different websites.
	Hide Artifacts: Hidden Window	Magic Hound malware has a function to determine whether the C2 server wishes to execute the newly dropped file in a hidden window.
	Indicator Removal on Host: File Deletion	Magic Hound has deleted and overwrote files to cover tracks.
	Ingress Tool Transfer	Magic Hound has downloaded additional code and files from servers onto victims.
	Input Capture: Keylogging	Magic Hound malware is capable of keylogging.
	Non-Standard Port	Magic Hound malware has communicated with its C2 server over TCP port 443 using HTTP.

	Obfuscated Files or Information	Magic Hound malware has used base64-encoded commands and files, and has also encrypted embedded strings with AES.
	OS Credential Dumping: LSASS Memory	Magic Hound stole domain credentials from Microsoft Active Directory Domain Controller and leveraged Mimikatz.
	Phishing: Spearphishing Link	Magic Hound sent shortened URL links over email to victims. The URLs linked to Word documents with malicious macros that execute PowerShells scripts to download Pupy.
	Phishing: Spearphishing via Service	Magic Hound used various social media channels to spearphish victims.
	Process Discovery	Magic Hound malware can list running processes.
	Screen Capture	Magic Hound malware can take a screenshot and upload the file to its C2 server.
	System Information Discovery	Magic Hound malware has used a PowerShell command to check the victim system architecture to determine if it is an x64 machine. Other malware has obtained the OS version, UUID, and computer/host name to send to the C2 server.
	System Network Configuration Discovery	Magic Hound malware gathers the victim's local IP address, MAC address, and external IP address.

	System Owner/User Discovery		Magic Hound malware has obtained the victim username and sent it to the C2 server.
	Web Service: Bidirectional Communication		Magic Hound malware can use a SOAP Web service to communicate with its C2 server.
Operations performed	**Date**	**Name**	**Target & Method**
	2014	Operation “Thamar Reservoir”	**Target:** 550 targets, most of them in the Middle East, from various fields: research about diplomacy, Middle East and Iran, international relations, and other fields; Defense and security; Journalism and human rights. **Method:** Breaching trusted websites to set up fake pages, Multi-stage malware, Multiple spear phishing emails based on reconnaissance and information gathering.
	Jan 2017	PupyRAT campaign	**Target:** Saudi financial, oil, and technology organizations. **Method:** Used shortened URLs in the body of the phishing emails.
	Oct 2018	The Return of The Charming Kitten	**Target:** Individuals who are involved in economic and military sanctions against the Islamic Republic of Iran as well as politicians, civil and human rights activists and journalists around the world. **Method:** Phishing attacks through email or social media and messaging accounts of public figures, which have been hacked by the attackers
	Jul 2019	The Kittens Are Back in Town	**Target:** Non-Iranian Researchers from the US, Middle East, and France, focusing on academic research of Iran, and Iranian dissidents in the US. **Method:** The first stage is sending an email message leveraging social engineering methods. The second stage includes a decoy website impersonating various Google services such as Gmail or Google Drive, to which the victim is redirected from the phishing email. Identified a

			new vector of phishing websites that is used by this group impersonating the Instagram official website.
	Late 2020	Operation “BadBlood”	**Target:** US and Israeli Medical Research Personnel Credential. **Method:** Phishing Campaigns.
	Jan 2021	Operation “SpoofedScholars”	**Target:** Individuals of intelligence interest to the Iranian government. **Method:** The use of a legitimate but actor-compromised website is an increase in sophistication compared to TA453’s historical Tactics, Techniques, and Procedures of using actor-controlled credential phishing websites.

Name	Molerats -> (FireEye)
Other Names	Extreme Jackal -> (CrowdStrike) Gaza Cybergang -> (Kaspersky) Gaza Hackers Team -> (Kaspersky) TA402 -> (Proofpoint) Aluminum Saratoga -> (SecureWorks) ATK 89 -> (Thales) TAG-CT5 -> (Google)
Country	🇵🇸 Gaza
First seen	2012
Description	The Gaza cybergang is an Arabic-language, politically-motivated cybercriminal group, operating since 2012 and actively targeting the MENA (Middle East North Africa) region. The Gaza cybergang's attacks have never slowed down and its typical targets include government entities/embassies, oil and gas, media/press, activists, politicians, and diplomats. The Gaza cybergang is sponsored by Hamas.
Targets	**Sectors:** Aerospace, Defense, Embassies, Energy, Financial, Government, High-Tech, Media, Oil and gas, Telecommunications and journalists and software developers. **Countries:** Afghanistan, Algeria, Canada, China, Chile, Denmark, Egypt, Germany, India, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Latvia, Libya, Macedonia, Morocco, New Zealand, Oman, Palestine, Qatar, Russia, Saudi Arabia, Serbia, Slovenia, Somalia, South Korea, Syria, Turkey, UAE, UK, USA, Yemen and the BBC and the Office of the Quartet Representative.
Tools used	**DropBook** [(https://attack.mitre.org/software/S0547/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=DropBook)] **DustySky** [(https://attack.mitre.org/software/S0062/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=DustySky)] **MoleNet** [(https://attack.mitre.org/software/S0553/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=MoleNet)]

	SharpStage [(https://attack.mitre.org/software/S0546/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=SharpStage)] **Spark** [(https://attack.mitre.org/software/S0543/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Spark)]	
Techniques used	**Name**	**Use**
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Molerats saved malicious files within the AppData and Startup folders to maintain persistence.
	Command and Scripting Interpreter: PowerShell	Molerats used PowerShell implants on target machines.
	Command and Scripting Interpreter: Visual Basic	Molerats used various implants, including those built with VBScript, on target machines.
	Command and Scripting Interpreter: JavaScript	Molerats used various implants, including those built with JS, on target machines.
	Credentials from Password Stores: Credentials from Web Browsers	Molerats used the public tool BrowserPasswordDump10 to dump passwords saved in browsers on victims.
	Deobfuscate/Decode Files or Information	Molerats decompresses ZIP files once on the victim machine.
	Ingress Tool Transfer	Molerats used executables to download malicious files from different sources.
	Obfuscated Files or Information	Molerats has delivered compressed executables within ZIP files to victims.
	Phishing: Spearphishing Attachment	Molerats has sent phishing emails with malicious Microsoft Word and PDF attachments.

	Phishing: Spearphishing Link	Molerats has sent phishing emails with malicious links included.
	Process Discovery	Molerats actors obtained a list of active processes on the victim and sent them to C2 servers.
	Scheduled Task/Job: Scheduled Task	Molerats has created scheduled tasks to persistently run VBScripts.
	Signed Binary Proxy Execution: Msiexec	Molerats has used msiexec.exe to execute an MSI payload.
	Subvert Trust Controls: Code Signing	Molerats has used forged Microsoft code-signing certificates on malware.
	User Execution: Malicious Link	Molerats has sent malicious links via email trick users into opening a RAR archive and running an executable.
	User Execution: Malicious File	Molerats has sent malicious files via email that tricked users into clicking Enable Content to run an embedded macro and to download malicious archives.

Operations performed	**Date**	**Name**	**Target & Method**
	Oct 2012	Operation "Molerats"	**Target:** Palestinian and Israeli surveillance targets, Government departments in Israel, Turkey, Slovenia, Macedonia, New Zealand, Latvia, the U.S., and the UK, The Office of the Quartet Representative, The British Broadcasting Corporation (BBC), A major U.S. financial institution, Multiple European government organizations. **Method:** Malicious download URL was sent to a well-known European government organization. The shortened URL breaks out to "http://lovegame[.]us/ Photos[.]zip," which was clicked/downloaded by the victim. Word

			document and installs/executes the Xtreme RAT binary into a temp directory, "Documents and Settings\admin\Local Settings\Temp\Chrome.exe." The decoy document, "rotab.doc," contains three images (a political cartoon and two edited photos), all negatively depicting former military chief Abdel Fattah el-Sisi. Xtreme RAT binary dropped: "Chrome.exe" (MD5: a90225a88ee974453b93ee7f0d93b104), which is unsigned. As of 29 May, the URL has been clicked 225 times by a variety of platforms and browser types, so the campaign was likely not limited to just one victim.
	Sep 2015	Operation "DustySky"	**Target:** Targeted sectors include governmental and diplomatic institutions, including embassies; companies from the aerospace and defense Industries; financial institutions; journalists; software developers **Method:** The attackers would usually send a malicious email message that either links to an archive file (RAR or ZIP compressed) or has one attached to it.
	Sep 2017	Operation "TopHat"	**Target:** Individuals or organizations within the Palestinian Territories **Method:** The first technique encountered included the use of malicious RTFs that made a HTTP request to which then redirected to the malicious site, the second technique uses an interesting tactic that, it makes use of an attack called Don't Kill My Cat or DKMC. DKMC can enable an attacker to load a legitimate bitmap (BMP) file that contains shellcode within it.
	Jan 2019	"Spark" Campaign	**Target:** Palestinian individuals and entities, likely related to the Palestinian government. **Method:** Used social engineering to infect victims, mainly from the Palestinian territories, with the Spark backdoor.
	Apr 2019	Operation "SneakyPastes"	**Target:** Politicians, diplomats, journalists, activists, and the region's other politically active citizens in the Middle East and countries in central Asia.

			Method: The campaign is multistage. It begins with phishing, using letters from one-time addresses and one-time domains. Sometimes the letters contain links to malware or infected attachments. If the victim executes the attached file (or follows the link), their device receives Stage One malware programmed to activate the infection chain.
	Dec 2019	"Pierogi" Campaign	**Target:** Entities and individuals in the Palestinian territories. **Method:** Used social engineering attacks to infect victims with a new, undocumented backdoor dubbed Pierogi and used different TTPs and decoy documents reminiscent of previous campaigns by MoleRATs involving the Micropsia and Kaperagent malware.

Name	APT 3 -> (Mandiant)
Other Names	Gothic Panda -> (CrowdStrike) Buckeye -> (Symantec) TG-0110 -> (SecureWorks) Bronze Mayfair -> (SecureWorks) UPS Team -> (Symantec) Group 6 -> (Talos)
Country	🇨🇳 China
First seen	2007
Description	Entities and individuals in the Palestinian territorie APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. APT3 utilizes a broad range of tools and techniques including spear-phishing attacks, zero-day exploits, and numerous unique and publicly available remote access tools (RAT). Victims of APT3 intrusions include companies in the defense, telecommunications, transportation, and advanced technology sectors — as well as government departments and bureaus in Hong Kong, the U.S., and several other countries.
Targets	**Sectors:** Aerospace, Construction, Defense, High-Tech, Manufacturing, Technology, Telecommunications, Transportation. **Countries:** Belgium, Hong Kong, Italy, Luxembourg, Philippines, Sweden, UK, USA, Vietnam.
Tools used	**LaZagne** [(https://attack.mitre.org/software/S0349/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=LaZagne)] **OSInfo** [(https://attack.mitre.org/software/S0165/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=OSInfo)] **PlugX** [(https://attack.mitre.org/software/S0013/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=PlugX)]

	RemoteCMD [(https://attack.mitre.org/software/S0166/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=RemoteCMD)]	
Techniques used	**Name**	**Use**
	Account Discovery: Local Account	APT3 has used a tool that can obtain info about local and global group users, power users, and administrators.
	Account Manipulation	APT3 has been known to add created accounts to local admin groups to maintain elevated Access.
	Archive Collected Data: Archive via Utility	APT3 has used tools to compress data before exfilling it.
	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT3 places scripts in the startup folder for persistence.
	Brute Force: Password Cracking	APT3 has been known to brute force password hashes to be able to leverage plain text credentials.
	Command and Scripting Interpreter: PowerShell	APT3 has used PowerShell on victim systems to download and run payloads after exploitation.
	Command and Scripting Interpreter: Windows Command Shell	An APT3 downloader uses the Windows command "cmd.exe" /C whoami. The group also uses a tool to execute commands on remote computers.
	Create Account: Local Account	APT3 has been known to create or enable accounts, such as support_388945a0.
	Create or Modify System Process: Windows Service	APT3 has a tool that creates a new service for persistence.

	Credentials from Password Stores: Credentials from Web Browsers	APT3 has used tools to dump passwords from browsers.
	Data from Local System	APT3 will identify Microsoft Office documents on the victim's computer.
	Data Staged: Local Data Staging	APT3 has been known to stage files for exfiltration in a single location.
	Event Triggered Execution: Accessibility Features	APT3 replaces the Sticky Keys binary C:\Windows\System32\sethc.exe for persistence.
	Exfiltration Over C2 Channel	APT3 has a tool that exfiltrates data over the C2 channel.
	File and Directory Discovery	APT3 has a tool that looks for files and directories on the local file system.
	Hide Artifacts: Hidden Window	APT3 has been known to use -WindowStyle Hidden to conceal PowerShell windows.
	Hijack Execution Flow: DLL Side-Loading	APT3 has been known to side load DLLs with a valid version of Chrome with one of their tools.
	Indicator Removal on Host: File Deletion	APT3 has a tool that can delete files.
	Ingress Tool Transfer	APT3 has a tool that can copy files to remote machines.
	Input Capture: Keylogging	APT3 has used a keylogging tool that records keystrokes in encrypted files.

	Multi-Stage Channels	An APT3 downloader first establishes a SOCKS5 connection to 192.157.198[.]103 using TCP port 1913; once the server response is verified, it then requests a connection to 192.184.60[.]229 on TCP port 81.
	Non-Application Layer Protocol	An APT3 downloader establishes SOCKS5 connections for its initial C2.
	Obfuscated Files or Information	APT3 obfuscates files or information to help evade defensive measures.
	Software Packing	APT3 has been known to pack their tools.
	Indicator Removal from Tools	APT3 has been known to remove indicators of compromise from tools.
	OS Credential Dumping: LSASS Memory	APT3 has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig”.
	Permission Groups Discovery	APT3 has a tool that can enumerate the permissions associated with Windows groups.
	Process Discovery	APT3 has a tool that can list out currently running processes.
	Proxy: External Proxy	An APT3 downloader establishes SOCKS5 connections for its initial C2.
	Remote Services: Remote Desktop Protocol	APT3 enables the Remote Desktop Protocol for persistence. APT3 has also interacted with compromised systems to browse and copy files through RDP sessions.

	Remote Services: SMB/Windows Admin Shares	APT3 will copy files over to Windows Admin Shares (like ADMIN$) as part of lateral movement.
	Remote System Discovery	APT3 has a tool that can detect the existence of remote systems.
	Scheduled Task/Job: Scheduled Task	An APT3 downloader creates persistence by creating the following scheduled task: schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System".
	Signed Binary Proxy Execution: Rundll32	APT3 has a tool that can run DLLs.
	System Information Discovery	APT3 has a tool that can obtain information about the local system.
	System Network Configuration Discovery	A keylogging tool used by APT3 gathers network information from the victim, including the MAC address, IP address, WINS, DHCP server, and gateway.
	System Network Connections Discovery	APT3 has a tool that can enumerate current network connections.
	System Owner/User Discovery	An APT3 downloader uses the Windows command "cmd.exe" /C whoami to verify that it is running with the elevated privileges of "System."
	Unsecured Credentials: Credentials In Files	APT3 has a tool that can locate credentials in files on the file system such as those from Firefox or Chrome.

	Valid Accounts: Domain Accounts		APT3 leverages valid accounts after gaining credentials for use within the victim domain.
Operations performed	**Date**	**Name**	**Target & Method**
	Apr 2014	Operation “Clandestine Fox”	**Target:** Internet Explorer (IE) IE6 through IE11 version users. **Method:** Zero-day which is bypassed both ASLR and DEP.
	Nov 2014	Operation “Double Tap”	**Target:** Multiple organizations in the world. **Method:** Leveraged multiple exploits, targeting both CVE-2014-6332 and CVE-2014-4113.
	Jun 2015	Operation “Clandestine Wolf”	**Target:** Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications and Transportation industries. **Method:** Upon clicking the URLs provided in the phishing emails, targets were redirected to a compromised server hosting JavaScript profiling scripts. Once a target host was profiled, victims downloaded a malicious Adobe Flash Player SWF file and an FLV file, detailed below. This ultimately resulted in a custom backdoor known as SHOTPUT, detected by FireEye as Backdoor.APT.CookieCutter, being delivered to the victim’s system.

Name	APT 17 -> (Mandiant)
Other Names	Deputy Dog -> (iDefense) Tailgater Team -> (Symantec) Elderwood -> (Symantec) Elderwood Gang -> (Symantec) Sneaky Panda -> (CrowdStrike) SIG22 -> (NSA) Beijing Group -> (SecureWorks) Bronze Keystone -> (SecureWorks) TG-8153 -> (SecureWorks) TEMP.Avengers -> (FireEye) Dogfish -> (iDefense) ATK 2 -> (Thales)
Country	🇨🇳 China
First seen	2009
Description	APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. The targeted industry sectors include, but are not restricted to; defense, various defense supply chain manufacturers, human rights and non-governmental organizations (NGOs), and IT service providers. These attackers are systematic and re-use components of an infrastructure we have termed the “Elderwood platform”. The name “Elderwood” comes from a source code variable used by the attackers. This attack platform enables them to quickly deploy zero-day exploits. Attacks are deployed through spear phishing emails and also, increasingly, through Web injections in watering hole attacks.

Targets	**Sectors:** Defense, Education, Energy, Financial, Government, High-Tech, IT, Media, Mining, NGOs and lawyers. **Countries:** Belgium, China, Germany, Indonesia, Italy, Japan, Netherlands, Switzerland, Russia, UK, USA.
Tools used	**BLACKCOFFEE** [(https://attack.mitre.org/software/S0069/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=BlackCoffee)] **Briba** [(https://attack.mitre.org/software/S0204/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Briba)] **Gh0st RAT** [(https://attack.mitre.org/software/S0032/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Gh0st%20RAT)]

	Name	**Use**
Techniques used	Acquire Infrastructure: Web Services	APT17 has created profile pages in Microsoft TechNet that were used as C2 infrastructure.
	Establish Accounts	APT17 has created and cultivated profile pages in Microsoft TechNet. To make profile pages appear more legitimate, APT17 has created biographical sections and posted in forum threads.

	Date	**Name**	**Target & Method**
Operations performed	Jul 2012	Breach of Bit9	**Target:** Bit9, a company that provides software and network security services to the U.S. government and at least 30 Fortune 100 firms. **Method:** Used custom-made malicious software.
	Aug 2013	Operation “DeputyDog”	**Target:** Organizations in Japan. **Method:** Campaign leveraging the then recently announced zero-day CVE-2013-3893.
	Nov 2013	Operation “Ephemeral Hydra”	**Target:** Strategically important websites, known to draw visitors that are likely interested in national and international security policy. **Method:** Inserting a zero-day exploit into a strategically important website, known to draw

			visitors that are likely interested in national and international security policy.
	Aug 2017	Operation “RAT Cook”	**Target:** Companies such as Google, Facebook. **Method:** Spear-phishing attack using a Game of Thrones lure.

<table>
<tr><td><b>Name</b></td><td colspan="2">APT 18 -> (Mandiant)</td></tr>
<tr><td><b>Other Names</b></td><td colspan="2">Dynamite Panda -> (CrowdStrike)
TG-0416 -> (SecureWorks)
Wekby -> (Palo Alto)
Scandium -> (Microsoft)</td></tr>
<tr><td><b>Country</b></td><td colspan="2">🇨🇳 China</td></tr>
<tr><td><b>First seen</b></td><td colspan="2">2009</td></tr>
<tr><td><b>Description</b></td><td colspan="2">APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical.
The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of Hacking Team's Flash zero-day exploit.'</td></tr>
<tr><td><b>Targets</b></td><td colspan="2"><b>Sectors:</b> Aerospace, Construction, Defense, Education, Engineering, Healthcare, High-Tech, Telecommunications, Transportation and Biotechnology.
<b>Countries:</b> USA.</td></tr>
<tr><td><b>Tools used</b></td><td colspan="2"><b>gh0st RAT</b> [(https://attack.mitre.org/software/S0032/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Gh0st%20RAT)]
<b>hcdLoader</b> [(https://attack.mitre.org/software/S0071/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=hcdLoader)]
<b>HTTPBrowser</b> [(https://attack.mitre.org/software/S0070/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=HTTPBrowser)]
<b>Pisloader</b> [(https://attack.mitre.org/software/S0124/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Pisloader)]</td></tr>
<tr><td rowspan="3"><b>Techniques used</b></td><td><b>Name</b></td><td><b>Use</b></td></tr>
<tr><td>Application Layer Protocol: Web Protocols</td><td>APT18 uses HTTP for C2 communications.</td></tr>
<tr><td>Application Layer Protocol: DNS</td><td>APT18 uses DNS for C2 communications.</td></tr>
</table>

	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT18 establishes persistence via the HKCU\Software\Microsoft\Windows\CurrentVersion\Run key.
	Command and Scripting Interpreter: Windows Command Shell	APT18 uses cmd.exe to execute commands on the victim’s machine.
	External Remote Services	APT18 actors leverage legitimate credentials to log into external remote services.
	File and Directory Discovery	APT18 can list files information for specific directories.
	Indicator Removal on Host: File Deletion	APT18 actors deleted tools and batch files from victim systems.
	Ingress Tool Transfer	APT18 can upload a file to the victim’s machine.
	Obfuscated Files or Information	APT18 obfuscates strings in the payload.
	Scheduled Task/Job: At (Windows)	APT18 actors used the native at Windows task scheduler tool to use scheduled tasks for execution on a victim network.
	System Information Discovery	APT18 can collect system information from the victim’s machine.
	Valid Accounts	APT18 actors leverage legitimate credentials to log into external remote services.

Operations performed	**Date**	**Name**	**Target & Method**
	Jun 2015	APT18 Demonstrating Hustle	**Target:** Using DNS Requests as Command and Control Mechanism **Method:** Phishing with obfuscated variants of the HTTPBrowser tool.
	May 2016	Attacks using DNS Requests as Command and Control Mechanism	**Target:** Organizations in the USA. **Method:** Phishing with Pisloader dropper.

Name	Stone Panda -> (CrowdStrike)
Other Names	APT 10 -> (Mandiant) menuPass Team -> (Symantec) menuPass -> (Palo Alto) Red Apollo -> (PWC) CVNX -> (BAE Systems) Potassium -> (Microsoft) Hogfish -> (iDefense) Happyyongzi -> (FireEye) Cicada -> (Symantec) Bronze Riverside -> (SecureWorks) CTG-5938 -> (SecureWorks) ATK 41 -> (Thales) TA429 -> (Proofpoint) ITG01 -> (IBM)
Country	🇨🇳 China
First seen	2006
Description	Stone Panda is a threat group that appears to originate from China and has been active since since at least 2009. Stone Panda has targeted healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors globally, with an emphasis on Japanese organizations. In 2016 and 2017, the group is known to have targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.
Targets	**Sectors:** Aerospace, Defense, Energy, Financial, Government, Healthcare, High-Tech, IT, Media, Pharmaceutical, Telecommunications and MSPs.

	Countries: Australia, Belgium, Brazil, Canada, China, Finland, France, Germany, Hong Kong, India, Japan, Netherlands, Norway, Philippines, Singapore, South Africa, South Korea, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.	
Tools used	**certutil** [(https://attack.mitre.org/software/S0160/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=certutil)] **ChChes** [(https://attack.mitre.org/software/S0144/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=ChChes)] **EvilGrab** [(https://attack.mitre.org/software/S0152/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=EvilGrab%20RAT)] **Impacket** [(https://attack.mitre.org/software/S0357/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Impacket)] **Mimikatz** [(https://attack.mitre.org/software/S0002/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=Mimikatz)] **PlugX** [(https://attack.mitre.org/software/S0013/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=PlugX)] **PowerSploit** [(https://attack.mitre.org/software/S0194/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=PowerSploit)] **PsExec** [(https://attack.mitre.org/software/S0029/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=PsExec)] **Pwdump** [(https://attack.mitre.org/software/S0006/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=pwdump)] **QuasarRAT** [(https://attack.mitre.org/software/S0262/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=QuasarRAT)] **RedLeaves** [(https://attack.mitre.org/software/S0153/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=RedLeaves)] **SNUGRIDE** [(https://attack.mitre.org/software/S0159/), (https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=SNUGRIDE)]	
Techniques used	**Name**	**Use**
	Account Discovery: Domain Account	Stone Panda has used the Microsoft administration tool csvde.exe to export Active Directory data.

	Acquire Infrastructure: Domains	Stone Panda has registered malicious domains for use in intrusion campaigns.
	Archive Collected Data	Stone Panda has encrypted files and information before exfiltration.
	Archive via Utility	Stone Panda has compressed files before exfiltration using TAR and RAR.
	Automated Collection	Stone Panda has used the Csvde tool to collect Active Directory files and data.
	Command and Scripting Interpreter: PowerShell	Stone Panda uses PowerSploit to inject shellcode into PowerShell.
	Command and Scripting Interpreter: Windows Command Shell	Stone Panda executes commands using a command-line interface and reverse shell. The group has used a modified version of pentesting script wmiexec.vbs to execute commands. Stone Panda has used malicious macros embedded inside Office documents to execute files.
	Data from Local System	Stone Panda has collected various files from the compromised computers.
	Data from Network Shared Drive	Stone Panda has collected data from remote systems by mounting network shares with net use and using Robocopy to transfer data.
	Data Staged: Local Data Staging	Stone Panda stages data prior to exfiltration in multi-part archives, often saved in the Recycle Bin.

	Data Staged: Remote Data Staging	Stone Panda has staged data on remote MSP systems or other victim networks prior to exfiltration.
	Deobfuscate/Decode Files or Information	Stone Panda has used certutil in a macro to decode base64-encoded content contained in a dropper document attached to an email. The group has also used certutil -decode to decode files on the victim’s machine when dropping UPPERCUT.
	Dynamic Resolution: Fast Flux DNS	Stone Panda has used dynamic DNS service providers to host malicious domains.
	Exploitation of Remote Services	Stone Panda has used tools to exploit the ZeroLogon vulnerability (CVE-2020-1472).
	File and Directory Discovery	Stone Panda has searched compromised systems for folders of interest including those related to HR, audit and expense, and meeting memos.
	Hijack Execution Flow: DLL Search Order Hijacking	Stone Panda has used DLL search order hijacking.
	Hijack Execution Flow: DLL Side-Loading	Stone Panda has used DLL side-loading to launch versions of Mimikatz and PwDump6 as well as UPPERCUT.
	Indicator Removal on Host: File Deletion	A Stone Panda macro deletes files after it has decoded and decompressed them.

	Ingress Tool Transfer	Stone Panda has installed updates and new malware on victims.
	Input Capture: Keylogging	Stone Panda has used key loggers to steal usernames and passwords.
	Masquerading	Stone Panda has used esentutl to change file extensions to their true type that were masquerading as .txt files.
	Rename System Utilities	Stone Panda has renamed certutil and moved it to a different location on the system to avoid detection based on use of the tool.
	Match Legitimate Name or Location	Stone Panda has been seen changing malicious files to appear legitimate.
	Native API	Stone Panda has used native APIs including GetModuleFileName, lstrcat, CreateFile, and ReadFile.
	Network Service Scanning	Stone Panda has used tcping.exe, similar to Ping, to probe port status on systems of interest.
	Obfuscated Files or Information	Stone Panda has encoded strings in its malware with base64 as well as with a simple, single-byte XOR obfuscation using key 0x40.
	OS Credential Dumping: Security Account Manager	Stone Panda has used a modified version of pentesting tools wmiexec.vbs and secretsdump.py to dump credentials.

	OS Credential Dumping: NTDS	Stone Panda has used Ntdsutil to dump credentials.
	OS Credential Dumping: LSA Secrets	Stone Panda has used a modified version of pentesting tools wmiexec.vbs and secretsdump.py to dump credentials.
	Phishing: Spearphishing Attachment	Stone Panda has sent malicious Office documents via email as part of spearphishing campaigns as well as executables disguised as documents.
	Process Injection: Process Hollowing	Stone Panda has used process hollowing in iexplore.exe to load the RedLeaves implant.
	Proxy: External Proxy	Stone Panda has used a global service provider's IP as a proxy for C2 traffic from a victim.
	Remote Services: Remote Desktop Protocol	Stone Panda has used RDP connections to move across the victim network.
	Remote Services: SSH	Stone Panda has used Putty Secure Copy Client (PSCP) to transfer data.
	Remote System Discovery	Stone Panda uses scripts to enumerate IP ranges on the victim network. menuPass has also issued the command net view /domain to a PlugX implant to gather information about remote systems on the network.
	Scheduled Task/Job: Scheduled Task	Stone Panda has used a script (atexec.py) to execute a command on a target machine via Task Scheduler.

	Signed Binary Proxy Execution: InstallUtil	Stone Panda has used InstallUtil.exe to execute malicious software.
	System Network Configuration Discovery	Stone Panda has used several tools to scan for open NetBIOS nameservers and enumerate NetBIOS sessions.
	System Network Connections Discovery	Stone Panda has used “net use” to conduct connectivity checks to machines.
	Trusted Relationship	Stone Panda has used legitimate access granted to Managed Service Providers in order to access victims of interest.
	User Execution: Malicious File	Stone Panda has attempted to get victims to open malicious files such as Windows Shortcuts (.lnk) and/or Microsoft Office documents, sent via email as part of spearphishing campaigns.
	Valid Accounts	Stone Panda has used valid accounts including shared between Managed Service Providers and clients to move between the two environments.
	Windows Management Instrumentation	Stone Panda has used a modified version of pentesting script wmiexec.vbs, which logs into a remote machine using WMI.

Operations performed	**Date**	**Name**	**Target & Method**
	Sep 2016	Spear-phishing attack	**Target:** Japanese academics working in several areas of science, along with Japanese pharmaceutical and a US-based subsidiary of a Japanese manufacturing organizations. **Method:** The attackers spoofed several sender email addresses to send spear-phishing emails,

			most notably public addresses associated with the Sasakawa Peace Foundation and The White House.
	2017	Operation “Soft Cell”	**Target:** Global telecommunications providers. **Method:** -
	Jul 2018	Attack on the Japanese media sector	**Target:** Japanese media sector. **Method:** The group sent spear phishing emails containing malicious documents that led to the installation of the UPPERCUT backdoor. This backdoor is well-known in the security community as ANEL, and it used to come in beta or RC (release candidate) until recently.
	Mar 2019	Operation “A41APT”	**Target:** Automotive, Electronics, Engineering, General Trading Company, Government, Industrial Products, Managed Service Providers and Manufacturing Industriai **Method:** Attackers used publicly available tools and techniques in these attacks. Gathering information from machines on the network, stealing user names and passwords, potentially to provide them with further access to the victim network. WMIExec can be used for lateral movement and to execute commands remotely.

Conclusions

The most important point in cyber security attacks is that to analyze the techniques used until the attack took place, predict which hacker group the attack was made by, predict the next move of the hacker group and take measures for that move. In this report, there is research needed to facilitate the analysis of cyber security atacks of hacker groups targeting the aerospace industry.

References

[1] https://attack.mitre.org/groups/G0032/

[2] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Lazarus%20Group%2C%20Hidden%20Cobra%2C%20Labyrinth%20Chollima

[3] https://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack

[4] https://www.symantec.com/connect/blogs/trojankoredos-comes-unwelcomed-surprise

[5] https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html

[6] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know

[7] https://unit42.paloaltonetworks.com/unit42-the-blockbuster-sequel/

[8] https://securelist.com/operation-applejeus/87553/

[9] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/

[10] https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf

[11] https://attack.mitre.org/groups/G0067/

[12] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Reaper%2C%20APT%2037%2C%20Ricochet%20Chollima%2C%20ScarCruft

[13] https://securelist.com/operation-daybreak/75100/

[14] https://unit42.paloaltonetworks.com/unit42-freemilk-highly-targeted-spear-phishing-campaign/

[15] https://attack.mitre.org/groups/G0003/

[16] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Cutting%20Kitten%2C%20TG%2D2889

[17] https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559

[18] https://www.secureworks.com/research/suspected-iran-based-hacker-group-creates-network-of-fake-linkedin-profiles

[19] https://attack.mitre.org/groups/G0087/

[20] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Chafer%2C%20APT%2039

[21] https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions

[22] https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/

[23] https://securelist.com/chafer-used-remexi-malware/89538/

[24] https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf

[25] https://attack.mitre.org/groups/G0059/

[26] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Magic%20Hound%2C%20APT%2035%2C%20Cobalt%20Gypsy%2C%20Charming%20Kitten

[27] https://www.clearskysec.com/thamar-reservoir/

[29] https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations

[29] https://blog.certfa.com/posts/the-return-of-the-charming-kitten/

[30] https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential

[31] https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453

[32] https://attack.mitre.org/groups/G0021/

[33] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Molerats%2C%20Extreme%20Jackal%2C%20Gaza%20Cybergang

[34] https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html

[35] https://unit42.paloaltonetworks.com/unit42-the-tophat-campaign-attacks-within-the-middle-east-region-using-popular-third-party-services/

[36] https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one

[37] https://www.kaspersky.com/blog/gaza-cybergang/26363/

[38] https://www.cybereason.com/blog/new-cyber-espionage-campaigns-targeting-palestinians-part-one

[39] https://attack.mitre.org/groups/G0022/

[40] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT%203%2C%20Gothic%20Panda%2C%20Buckeye

[41] https://www.fireeye.com/blog/threat-research/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html

[42] https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html

[43] https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

[44] https://attack.mitre.org/groups/G0025/

[45] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT%2017%2C%20Deputy%20Dog%2C%20Elderwood%2C%20Sneaky%20Panda

[46] https://www.fireeye.com/blog/threat-research/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

[47] https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html

[48] https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures

[49] https://attack.mitre.org/groups/G0026/

[50] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT%2018%2C%20Dynamite%20Panda%2C%20Wekby

[51] https://unit42.paloaltonetworks.com/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

[52] https://attack.mitre.org/groups/G0045/

[53] https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Stone%20Panda%2C%20APT%2010%2C%20menuPass

[54] https://unit42.paloaltonetworks.com/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/

[55] https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

[56] https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

[57] https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

[58] https://securelist.com/apt10-sophisticated-multi-layered-loader-ecipekac-discovered-in-a41apt-campaign/101519/

.