
FLASHBACK WITH
ATT&CK™
2003——2018
EXPLORING MALWARE HISTORY
WITH ATT&CK™

WHOIS

Kris Oosthoek

@f00th0ld

krisk.io

Threat Intelligence Analyst

rijkswaterstaat.nl/english

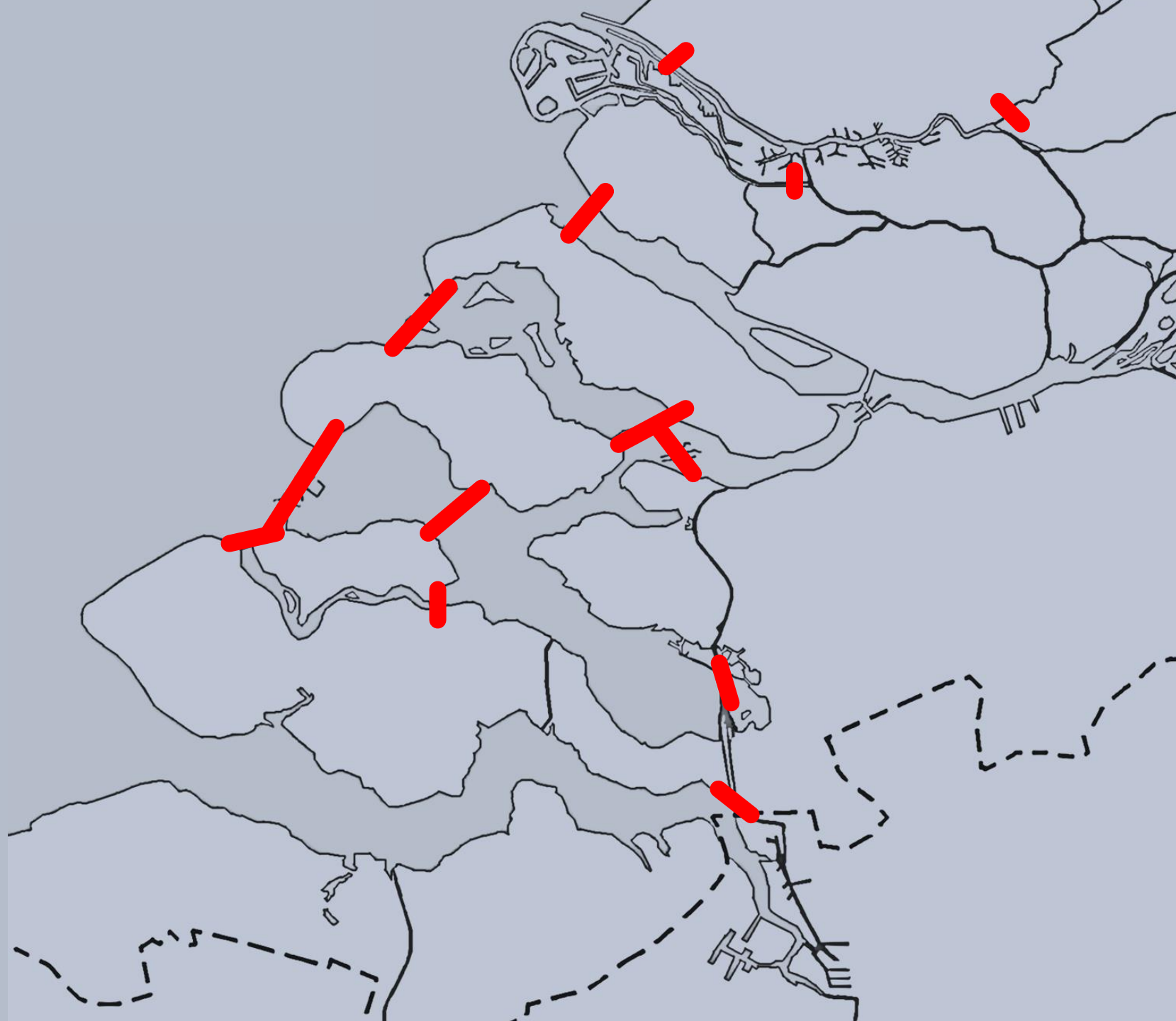
PhD Student

cyber-threat-intelligence.com

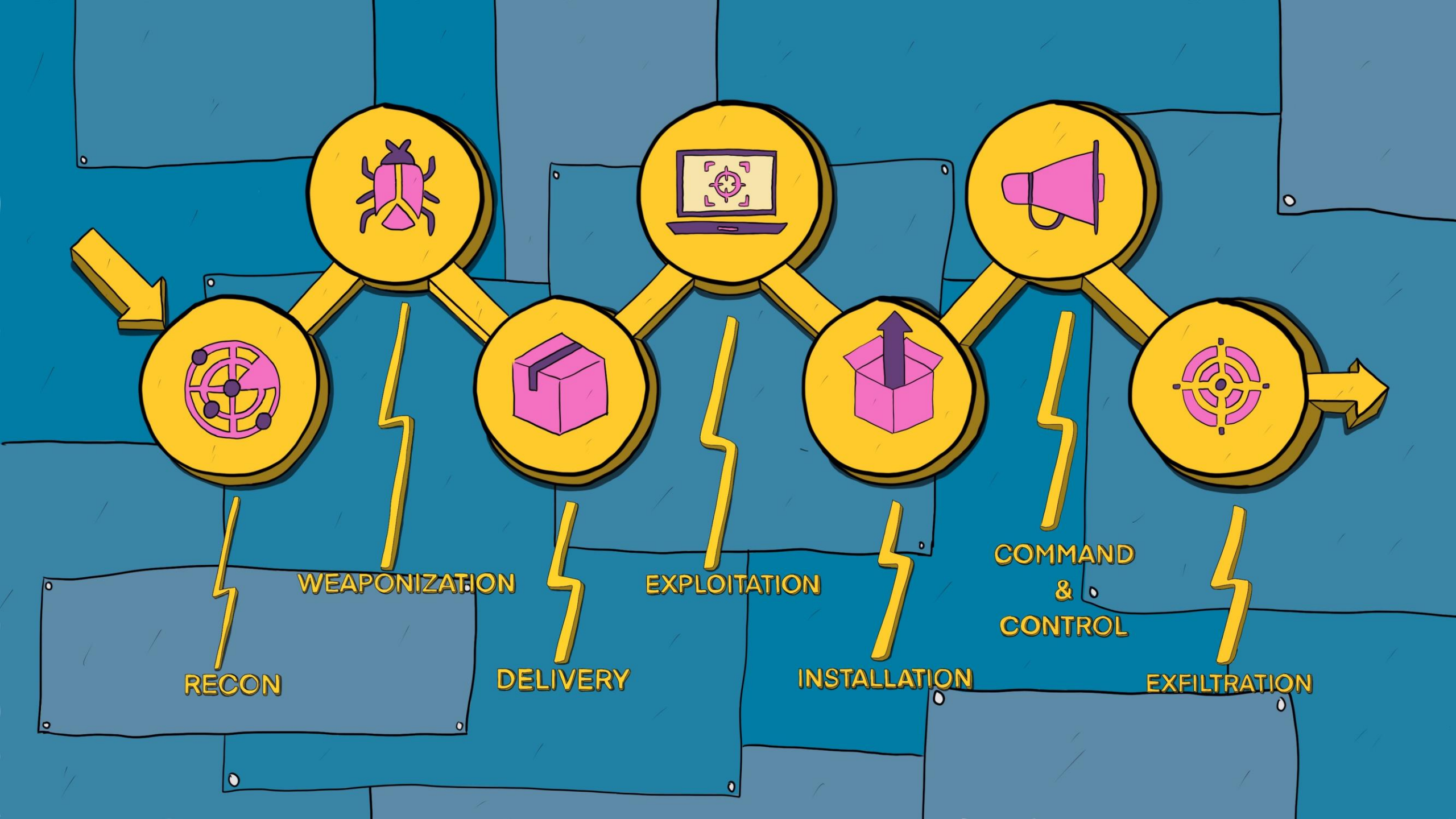
Overview

1. What/why
2. Methodology
3. Noteworthy findings
4. APT Technique Adoption
5. CTI from Automated Analysis

Kill Chain



wikipedia.org/wiki/Delta_Works


RECON
WEAPONIZATION
DELIVERY
EXPLOITATION
INSTALLATION
COMMAND & CONTROL
EXFILTRATION

What + why

- No articles *applying* ATT&CK in Google Scholar, IEEE, etc.

- **Aim¹:** stimulate academic adoption of ATT&CK
- **Aim²:** prove its potential for malware analysis
- **By:** plotting bulk analysis results on ATT&CK

Oosthoek, K., & Doerr, C. (2019). SoK: ATT&CK Techniques and Trends in Windows Malware. *Proceedings of SecureComm 2019, 15th EAI International Conference on Security and Privacy in Communication Networks*

TTPs

malpedia > VirusTotal JoeSecurity > ./jq >

951 samples

match SHA256 / automated analysis

ATT&CK plotting

data analysis

Initial Access	Execution	Persistence (1)	Persistence (2)	Privilege Escalation	Defence Evasion (1)	Defence Evasion (2)	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
Drive-by Compromise	CMSTP	Accessibility Features	Logon Scripts	Access Token Manipulation	Access Token Manipulation	Install Root Certificate	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	LSASS Driver	Accessibility Features	Binary Padding	InstallUtil	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	Modify Existing Service	AppCert DLLs	BITS Jobs	Masquerading	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Netsh Helper DLL	AppInit DLLs	Bypass User Account Control	Modify Registry	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	New Service	Application Shimming	CMSTP	Mshta	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Office Application Startup	Bypass User Account Control	Code Signing	Network Share Connection Removal	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	Path Interception	DLL Search Order Hijacking	Compiled HTML File	NTFS File Attributes	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Port Monitors	Exploitation for Privilege Escalation	Component Firmware	Obfuscated Files or Information	Hooking	Password Policy Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Redundant Access	Extra Window Memory Injection	Component Object Model Hijacking	Process Doppelgänging	Input Capture	Peripheral Device Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Registry Run Keys / Startup Folder	File System Permissions Weakness	Control Panel Items	Process Hollowing	Kerberoasting	Permission Groups Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	LSASS Driver	Component Firmware	Scheduled Task	Hooking	DCShadow	Process Injection	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Man in the Browser		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Screensaver	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Redundant Access	Network Sniffing	Query Registry	Taint Shared Content	Screen Capture		Multiband Communication
	PowerShell	Create Account	Security Support Provider	New Service	Disabling Security Tools	Regsvcs/Regasm	Password Filter DLL	Remote System Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvcs/Regasm	DLL Search Order Hijacking	Service Registry Permissions Weakness	Path Interception	DLL Search Order Hijacking	Regsvr32	Private Keys	Security Software Discovery	Windows Admin Shares			Remote Access Tools
	Regsvr32	External Remote Services	Shortcut Modification	Port Monitors	DLL Side-Loading	Rootkit	Two-Factor Authentication Interception	System Information Discovery	Windows Remote Management			Remote File Copy
	Rundll32	File System Permissions Weakness	SIP and Trust Provider Hijacking	Process Injection	Exploitation for Defense Evasion	Rundll32		System Network Configuration Discovery				Standard Application Layer Protocol
	Scheduled Task	Hidden Files and Directories	System Firmware	Scheduled Task	Extra Window Memory Injection	Scripting		System Network Connections Discovery				Standard Cryptographic Protocol
	Scripting	Hooking	Time Providers	Service Registry Permissions Weakness	File Deletion	Signed Binary Proxy Execution		System Owner/User Discovery				Standard Non-Application Layer Protocol
	Service Execution	Hypervisor	Valid Accounts	SID-History Injection	File Permissions Modification	Signed Script Proxy Execution		System Service Discovery				Uncommonly Used Port
	Signed Binary Proxy Execution	Image File Execution Options Injection	Web Shell	Valid Accounts	File System Logical Offsets	SIP and Trust Provider Hijacking		System Time Discovery				Web Service
	Signed Script Proxy Execution		Windows Management Instrumentation Event Subscription	Web Shell	Hidden Files and Directories	Software Packing						
	Third-party Software		Winlogon Helper DLL		Image File Execution Options Injection	Template Injection						
	Trusted Developer Utilities				Indicator Blocking	Timestomp						
	User Execution				Indicator Removal from Tools	Trusted Developer Utilities						
	Windows Management Instrumentation				Indicator Removal on Host	Valid Accounts						
	Windows Remote Management				Indirect Command Execution	Web Service						
	XSL Script Processing					XSL Script Processing						

Legend
950 observations
450 observations
300 observations
50 observations
10 observations

Execution

1. Execution Through API ▼
   - CreateProcessA / CreateProcessW functions
     found in 562 families
2. Rundll32
   - checking for system drives
     found in 175 families
3. Command-Line Interface ▲
   - popular for reverse shells; obfuscated CMDs
     found in 161 families
4. Service Execution ▼
   - binary, command or script
     found in 115 families, but significantly decreasing from 2012-2018
   - creating remote processes via PsExec
     Carbanak, Koadic, OlympicDestroyer, NetC

TL;DR: Execution techniques most commonly have a short lifecycle

Execution: Fileless Techniques

- PowerShell ▲

  PS command line, CreateObject for Execution
  7 families, all from either 2017 or 2018
  Emotet, Rozena, DNSMessenger, Ramnit, DownPaper, SnatchLoader, Empire

- Windows Management Instrumentation ▲

  checking for system drives
  82 families accessed WMI (configuration information), of which 7 using WMIC i.a. EternalPetya, LatentBot, ISFB, Dropshot, GhostRAT

TL;DR:

- Increasing proliferation of fileless Execution techniques
- At the expense of more established techniques

Defense Evasion

1. Obfuscated Files or Information	obfuscated instructions, .NET CreateDecryptor, found in 593 families
2. Software Packing	*zlib* compression, UPX, RAR found in 558 families
3. Deobfuscate/Decode Files or Information	string en-/decryption functions 359 families; encoding only malicious sections of file
4. Masquerading	Program Files, system32, driver directories found in 165 families, of which 19 masquerading as 3rd party software
5. DLL Side-Loading ▲	using legitimate applications to load DLLs 106 families, of which 90 first observed 2016-2018

TL;DR: implement hash-based DLL import validation

Discovery

1. Query Registry	AuthenticodeEnabled, query GUID 950 samples, of which 345 lookup GUID
2. Security Software Discovery ▲	check for AV, local FW rules, virtualization 748 families; several subtechniques (e.g. RDTSC instruction) on the rise
3. Process Discovery	CreateTool32Snapshot(), Process32First/Next() 599 families
4. System Information Discovery	GetVersion(), GetLocaleInfo(), VirtualQuery() observed in 669 families
5. System Network Configuration Discovery	GetAdaptersInfo(), ipconfig, netsh, netstat, GeoIP found in 97 families, of which 60 call GetAdaptersInfo()

TL;DR: well-detected but difficult to distinguish malicious from benign

Command and Control

1. Uncommonly Used Port

TCP/UDP with unexpected protocol behavior
observed in 67 families

2. Web Service

using Facebook, Tumbler, VKontakte, Pastebin
found in 47 families (AdKoob, Empire, OnionDuke, PlugX, yty)

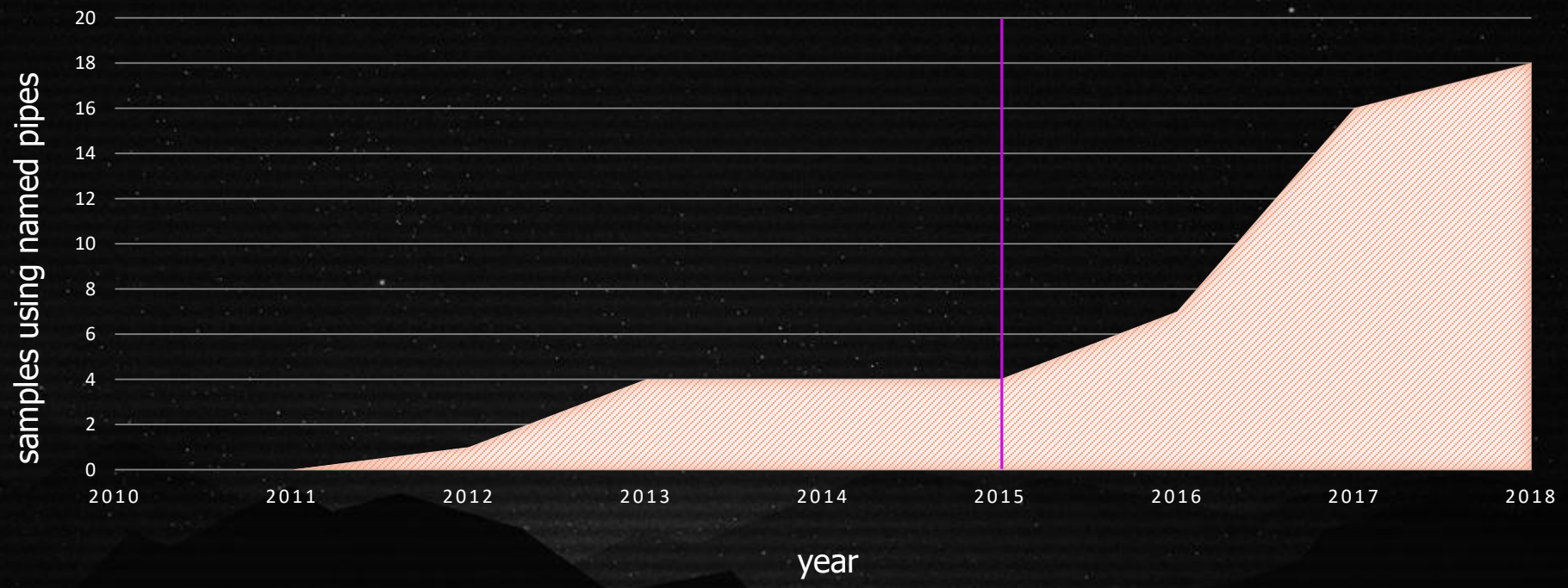
3. Multi-hop Proxy

C&C over TOR (connects to .onion)
found in 11 families (AthenaGo, WannaCryptor, Polyglot, XBot POS)

4. Process Injection

"More sophisticated samples may perform multiple process injections (…) utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel." https://attack.mitre.org/techniques/T1055

APT Technique Adoption



In depth: krisk.io/post/attack

Lessons Learned: CTI from Automation

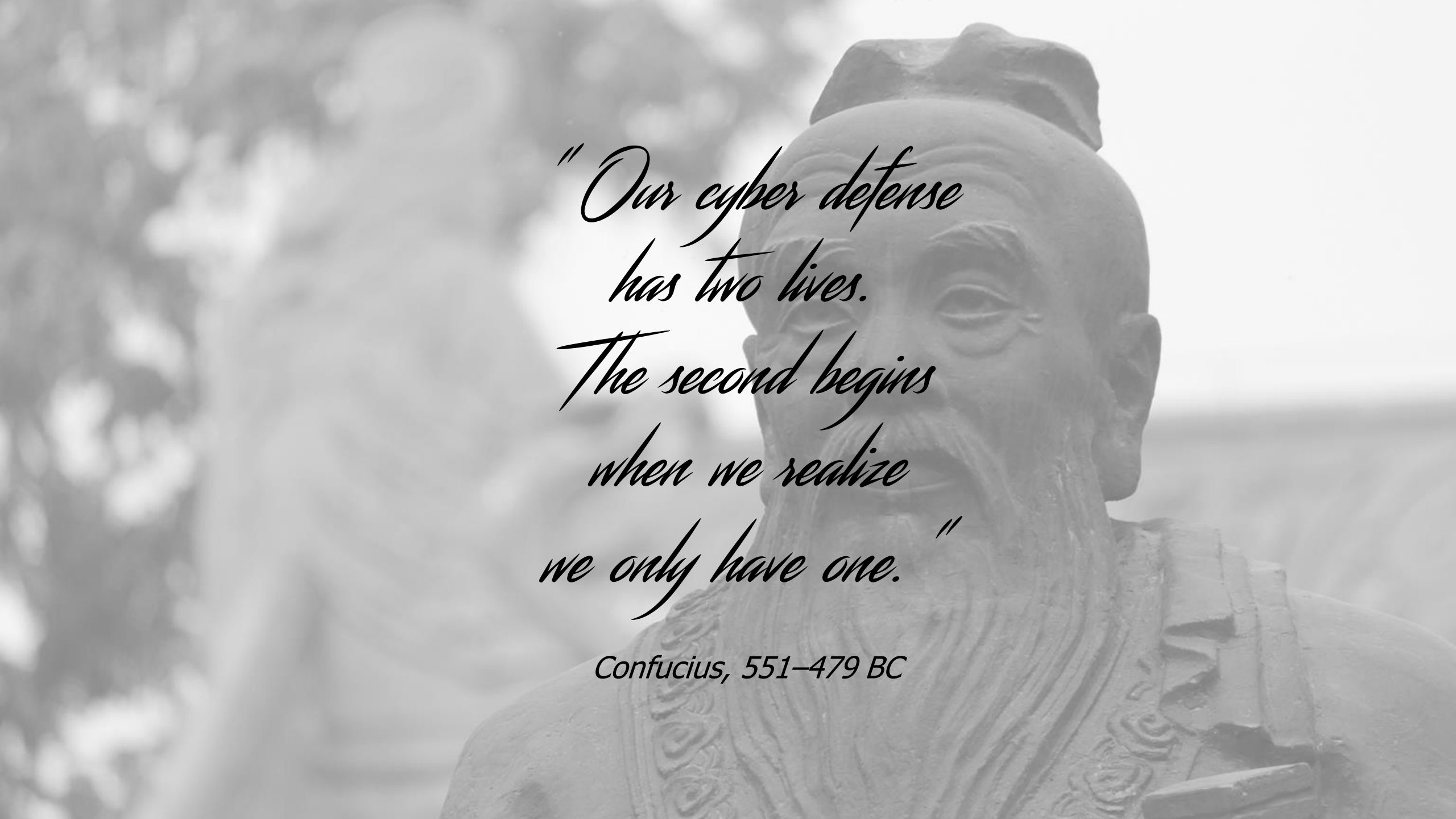
1 Inaccurate technique plotting

2 Partial and biased coverage of certain tactics

3 Results always depend on the capabilities of the resource used for analysis

>> Automated analysis is an unsuited source for CTI when taken by itself

- Critical thinking is the sharpest tool in your toolbox
- Always consider alternative hypotheses
- Curate carefully


"Our cyber defense
has two lives.
The second begins
when we realize
we only have one."
Confucius, 551–479 BC

Thanks!

Kris Oosthoek
@f00th0ld
krisk.io

TU Delft