RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **PART2-T10**

2020 ATT&CK™ Vision

Correlating TTPs to Disrupt Advanced Cyberattacks

Rick McElroy

Principal Cybersecurity Strategist
VMware Carbon Black
@InfoSecRick

Greg Foss

Senior Threat Researcher
VMware Carbon Black
@heinzarelli

RSAConference2020

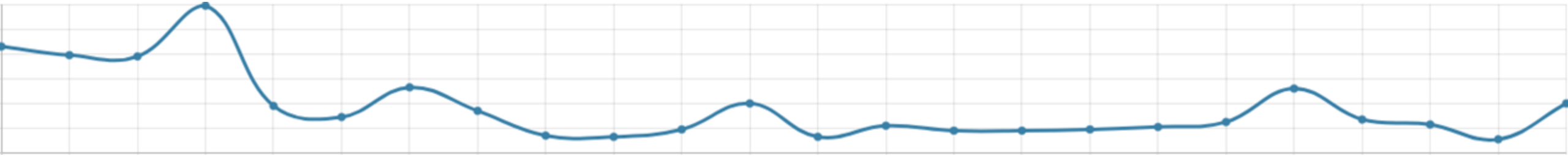
Profiling Malware using MITRE ATT&CK™

Understanding Common Techniques Tactics and Procedures

Profiling Malware using MITRE ATT&CK™

Research Goals:

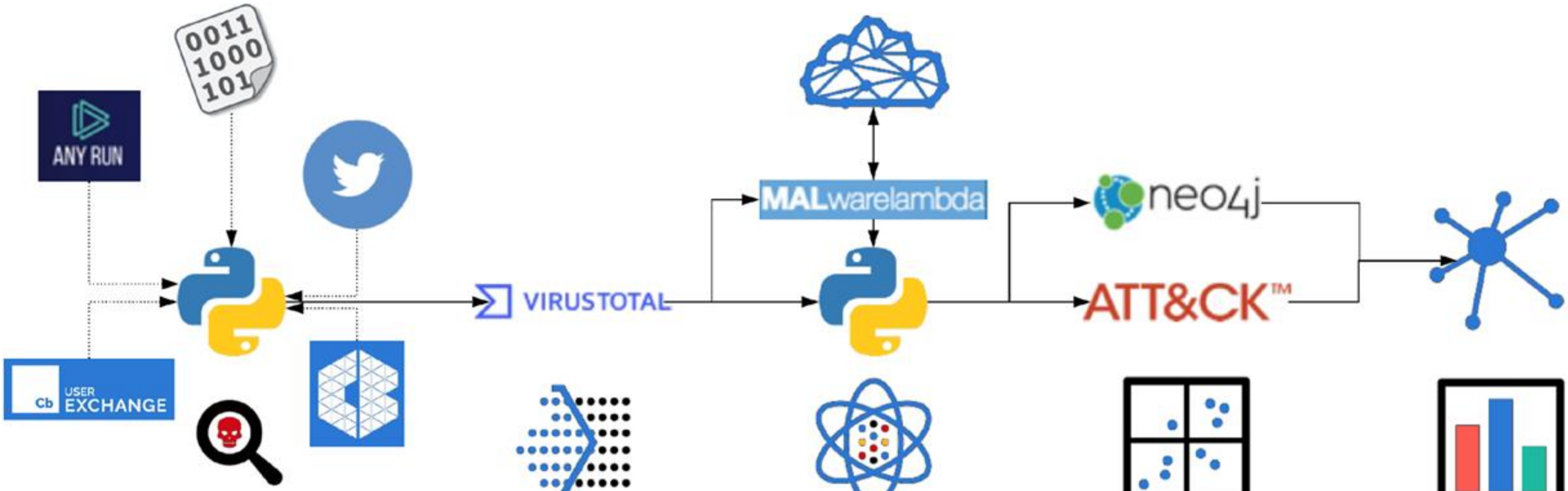
- Provide guidance on optimal security efficacy and prevention
- Reduce overall false positives that detract from detection efficacy
- Understand common TIDs associated with malware classifications
- Determine most prevalent techniques in use by modern malware
- Highlight edge-cases and outliers of unique Techniques



Why?

- Help the security community defend more effectively against all types of malware
- Separate fiction from fact through systematically analyzing a pool of malware families and presenting the findings
- Create a repeatable process to extend our analytics pipeline
- Understand trends and techniques that overlap among malware families, and utilize this information to adapt detections

MITRE ATT&CK™ – Malware Profiling



Malware Supply

- VMware Carbon Black Cloud
- VMware Carbon Black User Exchange
- AnyRun Public Sandbox
- TotalHash
- Twitter Scraping
- VirusTotal

Hash Processing and Normalization to SHA256

- Tag, Organize, and Convert Samples
- Validate all samples

Categorization and Dynamic Detonation

- Ensure all samples exist in database
- Detonate Samples
- Capture Static and Dynamic Data
- Utilize internal malware analysis environments within MalwareLambda
- Analyze telemetry and behavioral data from VMware Carbon Black Cloud

Data Processing and Analytics Output

- Correlate all collected data to MITRE ATT&CK and associate behavioral data to relevant TIDs
- Visualize and correlate relational data with Neo4j

Malware Profiles Mapped to MITRE ATT&CK

- Analyze collected data
- Extrapolate commonality of TIDs in relation to malware family
- Utilize data to improve security efficacy

Key Highlights

- Defense evasion behavior was seen in more than 90 percent of samples
- Ransomware has seen a significant resurgence over the past year
- Top Targeted Industries Include: Energy and Utilities, Government and Manufacturing
- Ransomware's evolution has led to more sophisticated Command and Control (C2)
- Wipers continue to trend upward
- Classic malware families have spawned the next generation

RSAConference2020

Destructive Malware

Ransomware, Wipers, and more...

History of Destructive Cyber Attacks

Subset of High Profile, Public, and Documented Destructive Attacks

Physically Destructive

Destructive

1980 | 1990 | 2000 | 2010

1982: Siberian Pipeline
The CIA tricked the Soviet Union into acquiring ICS software with built-in flaws. Software was programmed to malfunction - resulting in one of the worlds largest non-nuclear explosions.

1998: Kosovo
35,000 Computers wiped and replaced with burning American flag by Iranians.

1998: CIH
Chernobyl virus which overwrote critical system data – affecting 60-million computers. Developed by a Taiwanese Student.

2008: Beijing Olympics
Deceptive Russian Campaign to disrupt the Olympic Games.

2008: Georgia
Russian Joint campaign against Georgian targets. Website defacement, DDoS, and diverting citizens web traffic through Russia.

2010: Stuxnet
US and Israeli developed-malware leveraged to delay the Iranian Nuclear Program's ability to enrich Uranium. The malware targeted Siemens ICS and physically destroyed Uranium centrifuges, leveraging 4 zero-days.

2013: Dark Seoul
North Korean attacks on South Korean Television Stations and Banks.

2014: Sony Entertainment
North Korean attack in response to movie – data theft and wiping resulting in $35 million in damages.

2014: German Steel Mill
Attack on ICS controlling blast furnace, resulting in significant physical damage.

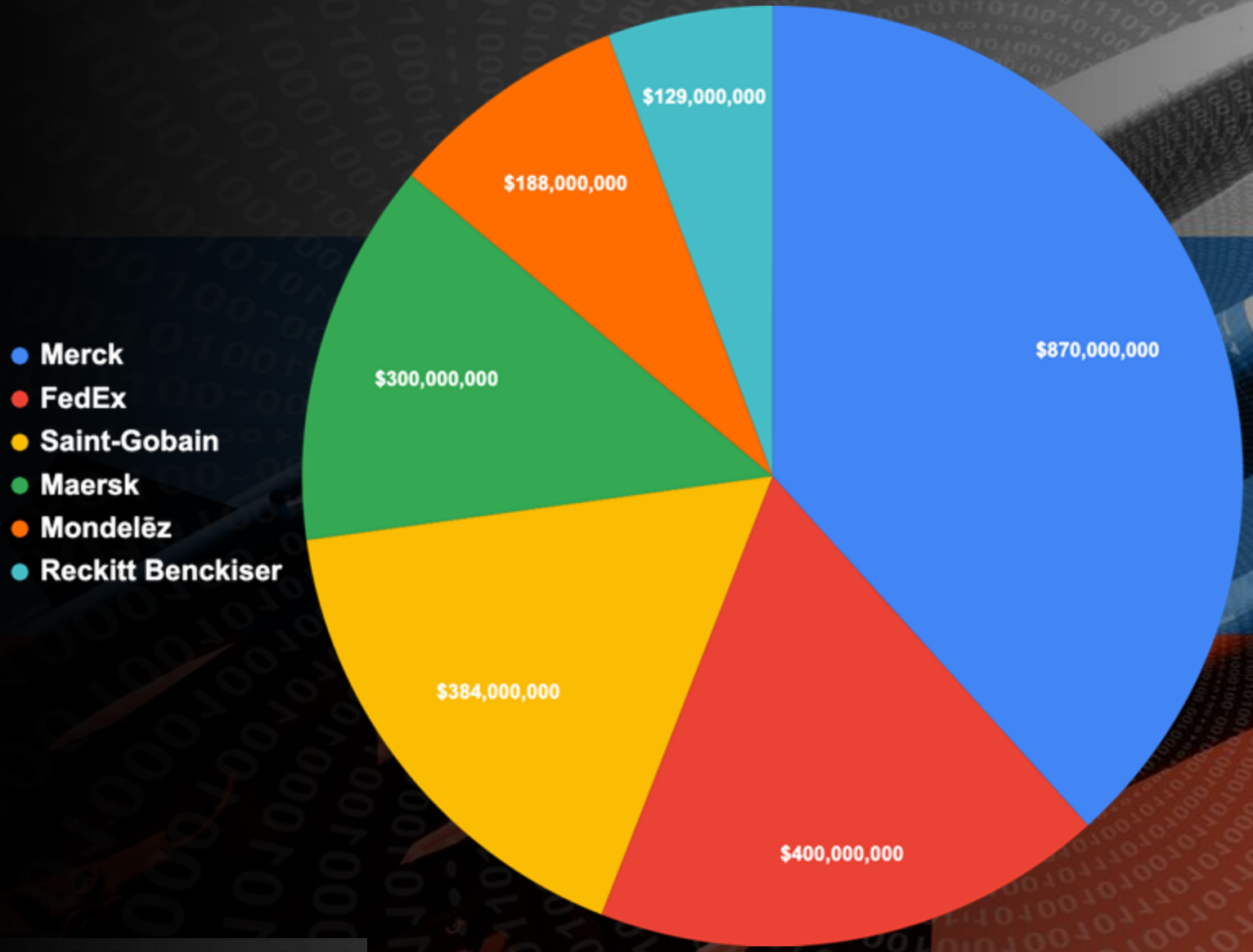
2015: TV5Monde
Russian actors destroyed French TV station hardware, taking the network offline for 12-hours.

2015: Black Energy
Russian attack on three Ukrainian Energy Distribution Companies. Cutting power to 750,000 civilians.

2016: Crash Override
Russian attack on electric transmission station ICS systems in Kiev, Ukraine.

2017: NotPetya
One of the most damaging Cyber Attacks in history. Russia targeted large Ukraine companies. Estimated to have cost over $10 Billion in damages, globally.

NotPetya - Financial Impact



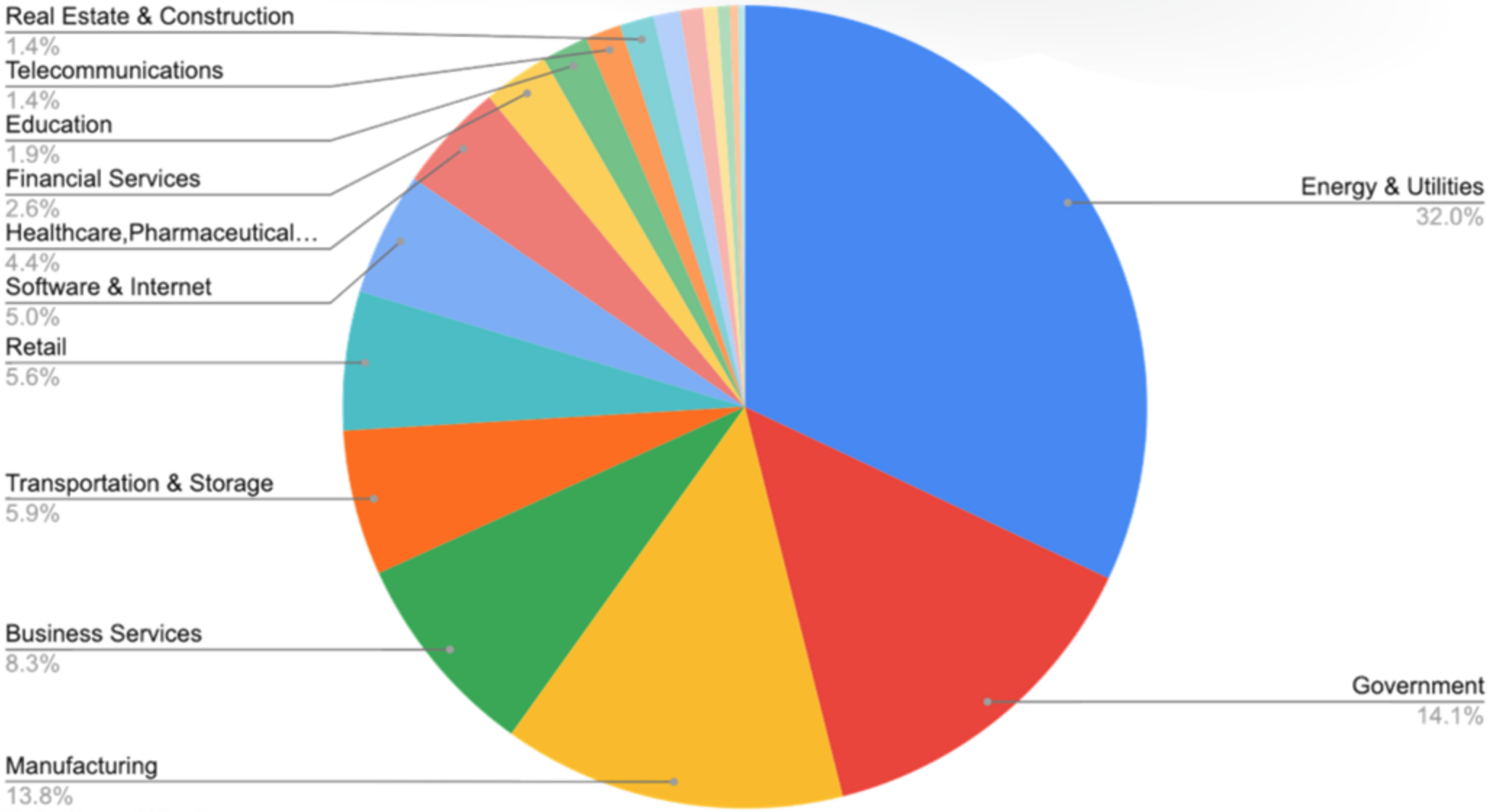
$7.5 Billion in damages to smaller companies

$10 billion

Total damages from NotPetya, as estimated by the White House

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

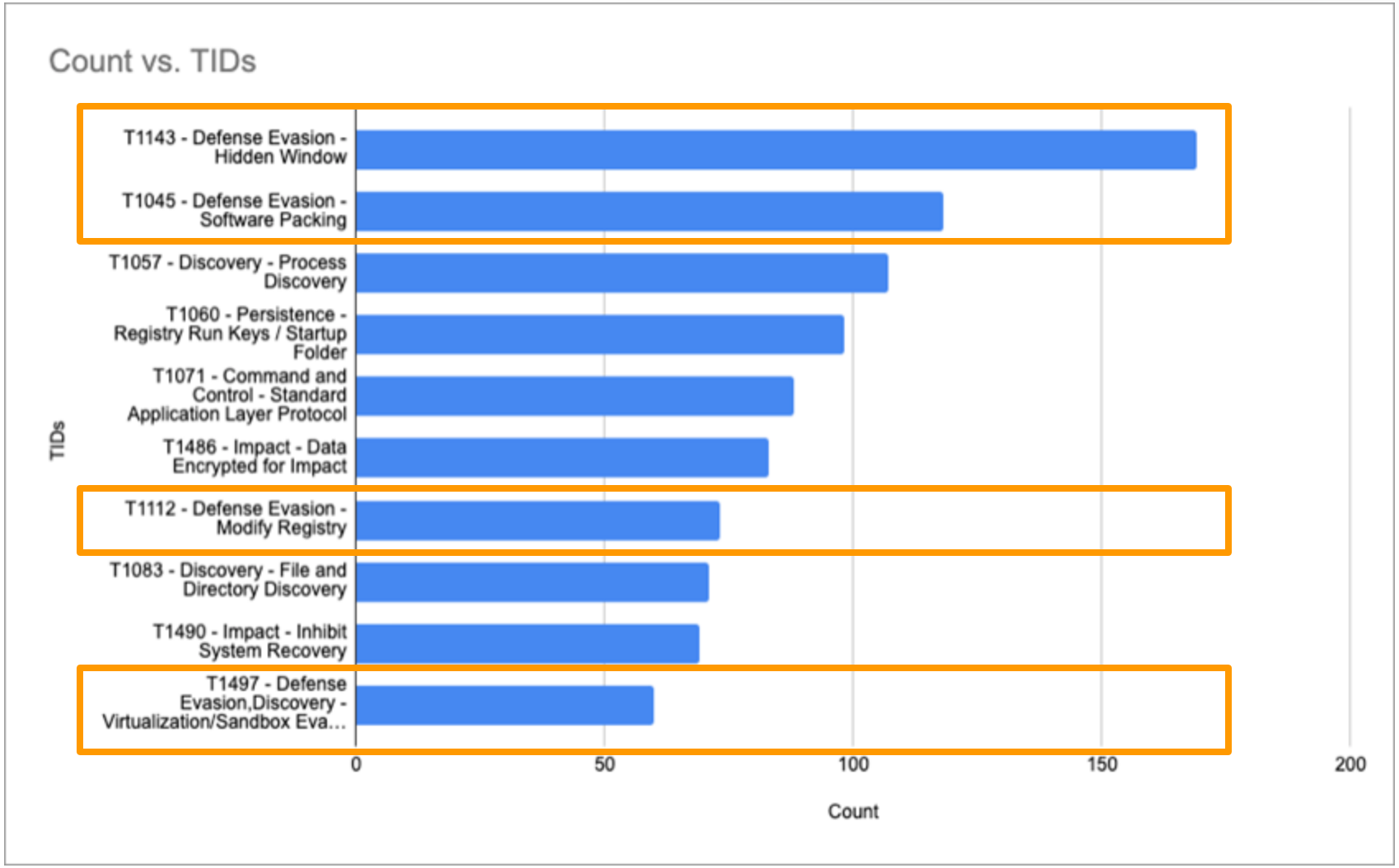
Distribution of Ransomware Across Industry Verticals



Ransomware ATT&CK'd

RANSOMWARE											
MITRE ATT&CK											
Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Command and Control**	**Exfiltration**	**Impact**
	Scripting	Hidden Files and Directories	New Service	Hidden Window	Credentials in Files	Virtualization/Sandbox Evasion	Remote File Copy	Data from Local System	Standard Application Layer Protocol		Data Encrypted for Impact
	Windows Management Instrumentation	Registry Run Keys / Startup Folder	Scheduled Task	Software Packing	Input Capture	Process Discovery		Automated Collection	Standard Cryptographic Protocol		Inhibit System Recovery
	Command-Line Interface	Bootkit	Hooking	Modify Registry	Hooking	File and Directory Discovery		Data from Network Shared Drive	Multilayer Encryption		Data Destruction
	Scheduled Task	New Service	Service Registry Permissions Weakness	Virtualization/Sandbox Evasion		System Time Discovery		Clipboard Data	Multi-hop Proxy		Defacement
		Scheduled Task		Hidden Files and Directories		System Network Configuration Discovery		Input Capture	Remote File Copy		Service Stop
		Hooking		Scripting		Query Registry					
		Service Registry Permissions Weakness		NTFS File Attributes		System Network Connections Discovery					
				Masquerading		System Information Discovery					
				File System Logical Offsets		Network Share Discovery					
				Obfuscated Files or Information		Security Software Discovery					
				Rootkit		Application Window Discovery					
				Disabling Security Tools							
				Indicator Removal on Host							
				File Deletion							

Ransomware Behaviors

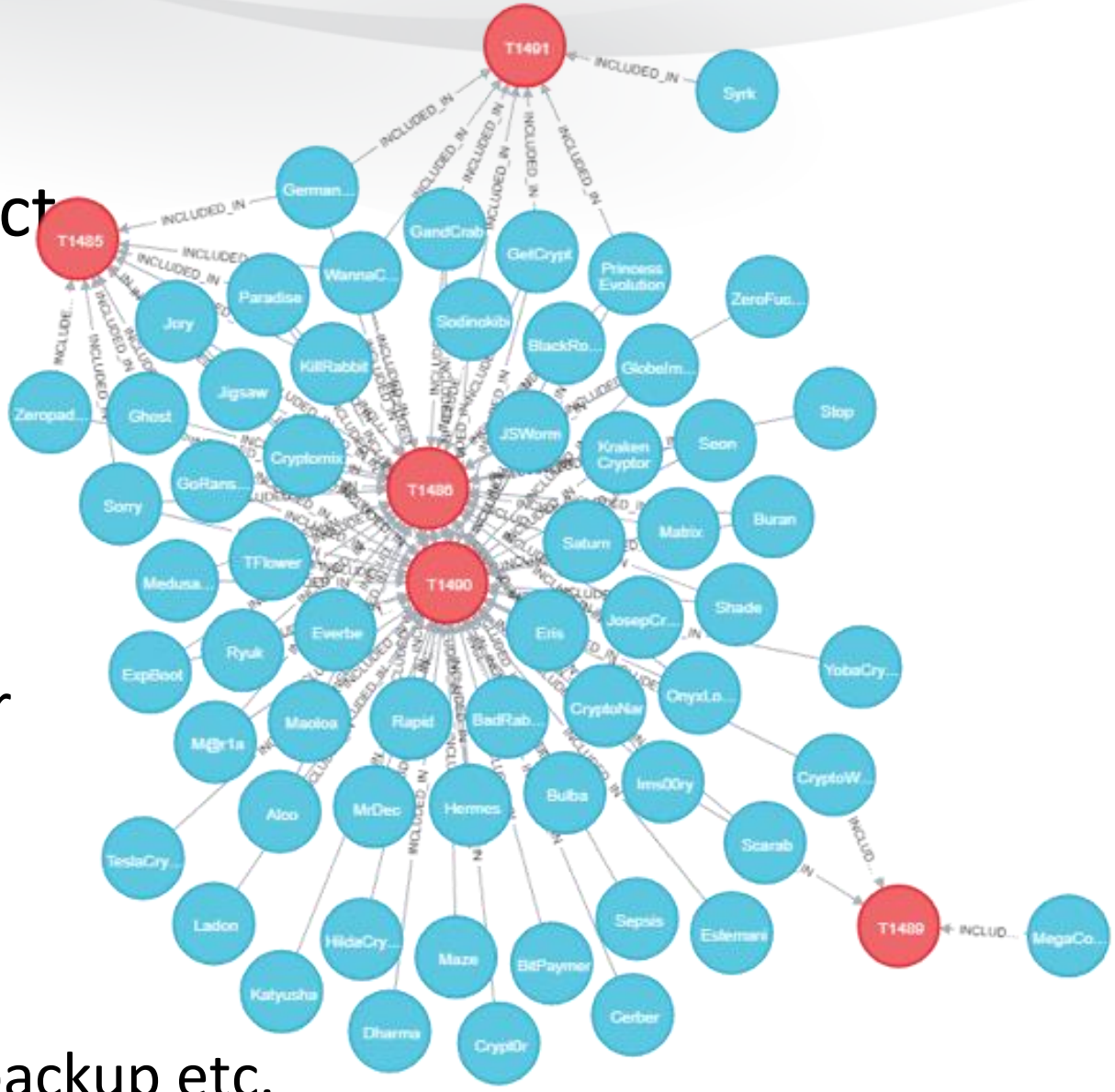


Ransomware - Defense Evasion

- T1497 – Virtualization / Sandbox Evasion
  - AV, backup, monitoring detection
- T1045 – Software Packing
  - UPX, ASPack, .NET obfuscaters etc.
- T1143 – Hidden Window
  - PowerShell
- T1036 – Masquerading
  - svchostt.exe, expllorer.exe

Ransomware - Impact

- T1486 – Data Encrypted for Impact
- T1490 – Inhibit System Recovery
  - vssadmin delete shadows, bcdedit
- T1485 – Data Destruction
  - Ransomware that also acts as a wiper
- T1491 – Defacement
- T1489 – Service Stop
  - Stopping of critical services e.g. AV, backup etc.

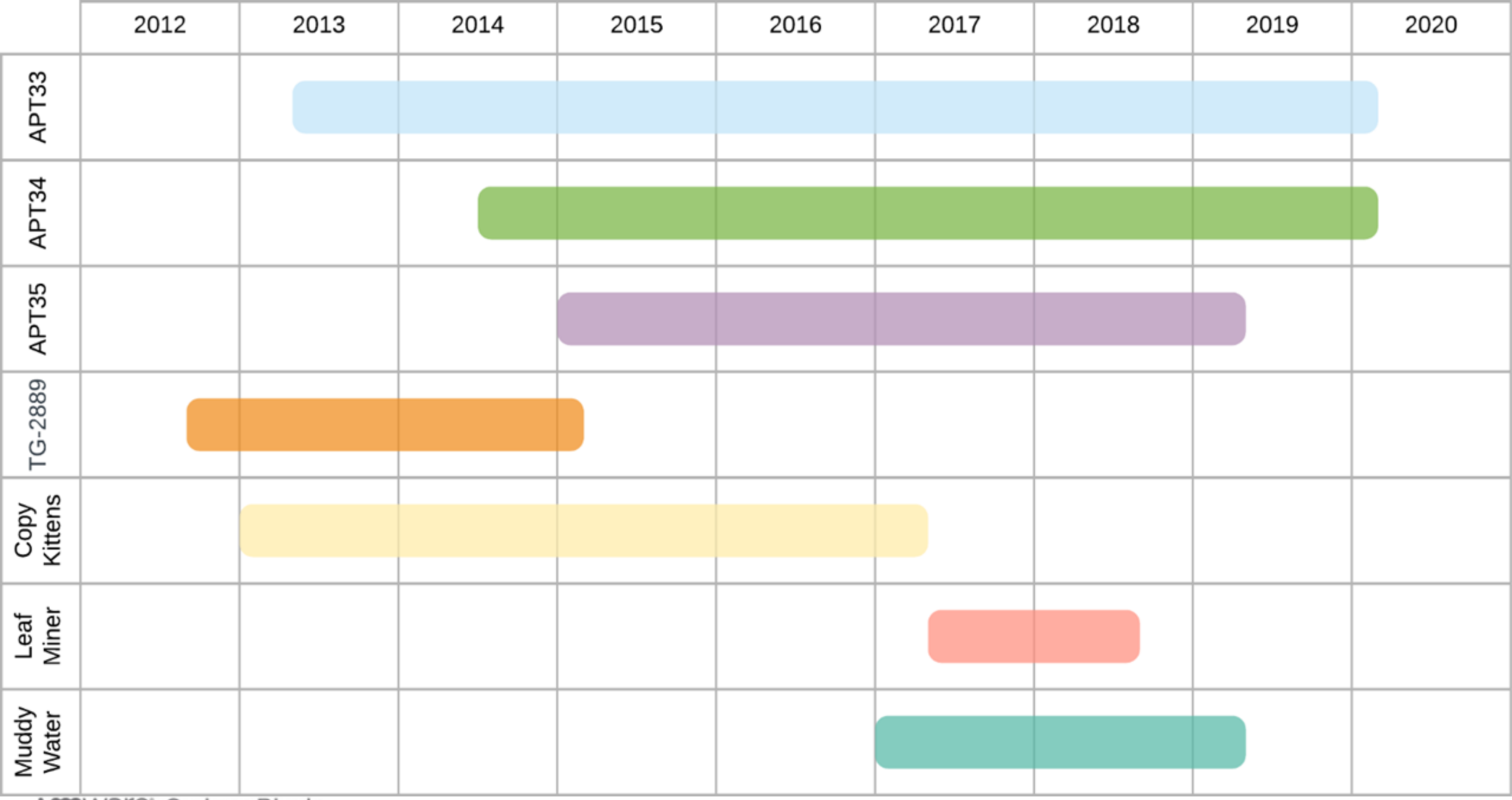


Ransomware Takeaways

- Defense Evasion is imperative to successful Ransomware infection
  - Software Packing, Sandbox Evasion, Masquerading, and Hidden Windows
- Various persistence methods are leveraged consistently
  - Hidden files/folders, scheduled tasks, registry mods, Bootkits, etc.
  - Persistence mechanisms often remain following decryption
- Credentials are accessed and leveraged for privilege escalation
  - Often exfiltrated over plain-text-protocols and used to maintain access

Ransomware turned Wiper…

- Reverse Engineering and repurposing of existing ransomware
  - NotPetya
- A continuing trend of creating ransomware with no actual decryption mechanism is being observed across the industry
  - Shamoon, GermanWiper, Dustman, etc…
- Nation States are increasingly leveraging wormable wipers
- When the goal is simply destruction – all bets are off…

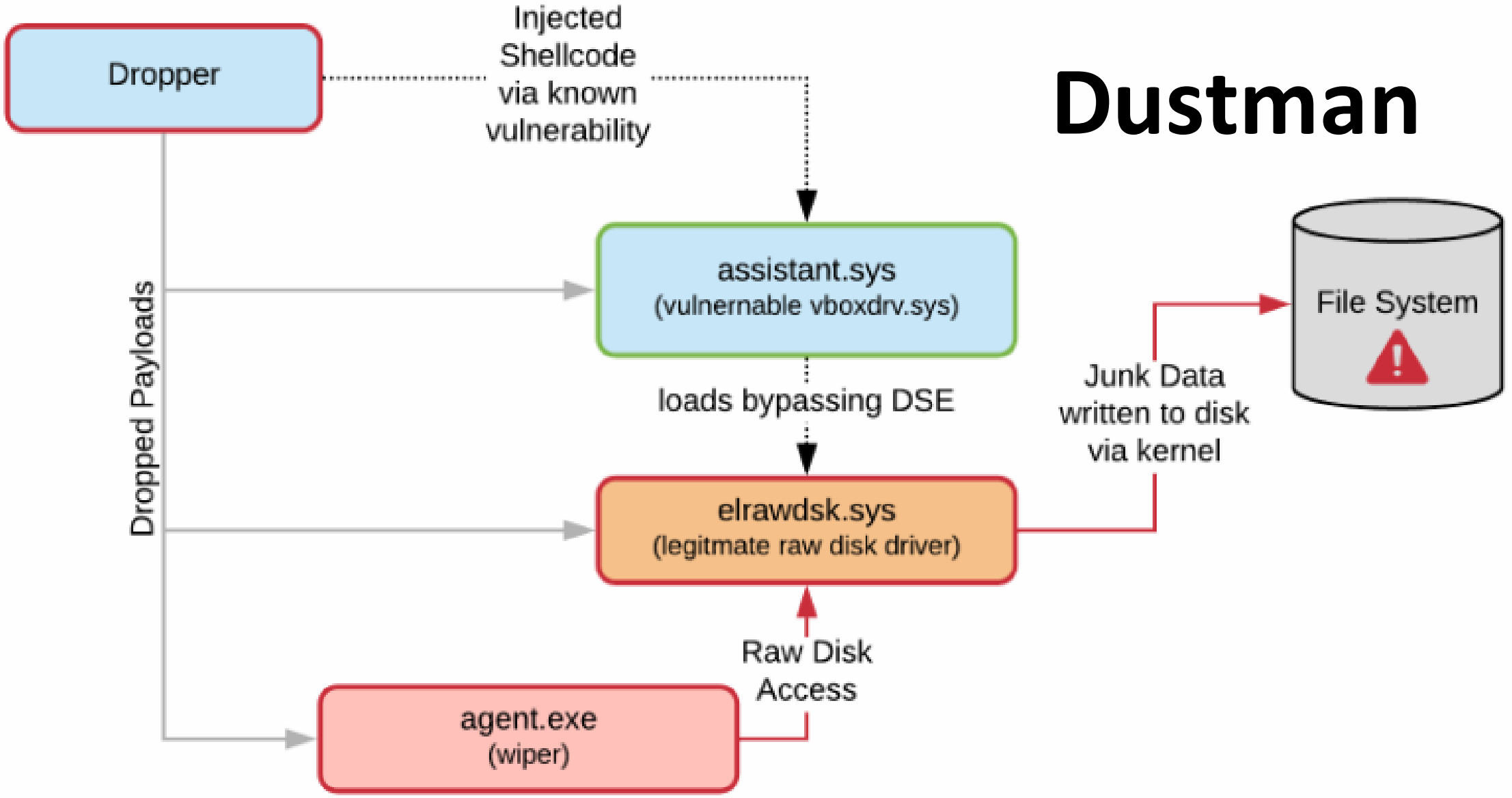

2012
2013
2014
2015
2016
2017
2018
2019
2020
APT33
APT34
APT35
TG-2889
Copy Kittens
Leaf Miner
Muddy Water

New Iranian data wiper malware hits Bapco, Bahrain's national oil company

Saudi Arabia's cyber-security agency spots new Dustman data-wiping malware.

By Catalin Cimpanu for Zero Day | January 9, 2020 -- 04:28 GMT (20:28 PST) | Topic: Security

Dustman

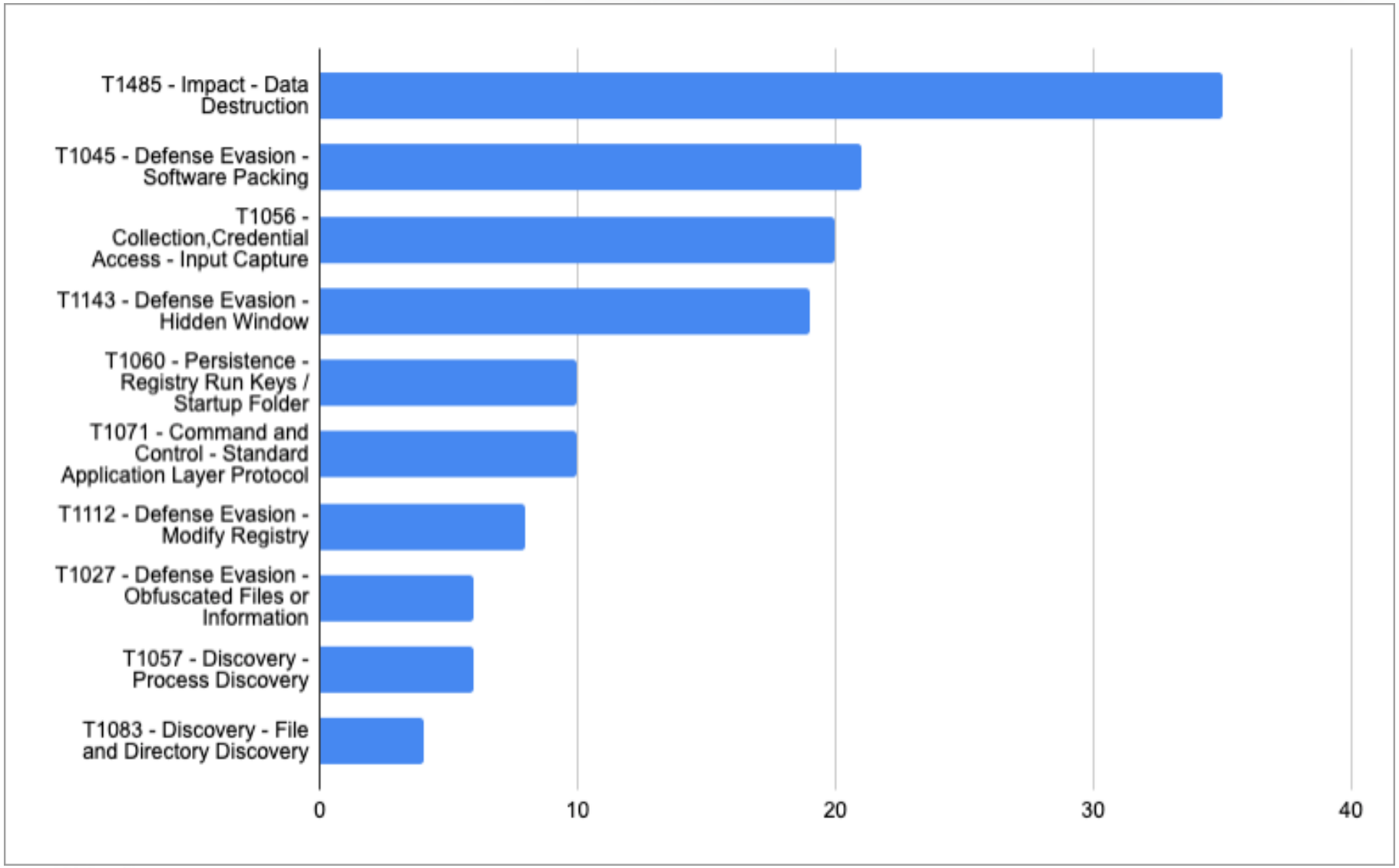


https://www.carbonblack.com/2020/01/21/threat-analysis-unit-tau-technical-report-the-prospect-of-iranian-cyber-retaliation/

Wipers ATT&CK'd

WIPERS											
MITRE ATT&CK											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Scheduled Task	Registry Run Keys / Startup Folder	New Service	Software Packing	Credentials in Files	Process Discovery	Remote File Copy	Data from Local System	Standard Application Layer Protocol		Data Destruction
		Bootkit	Scheduled Task	Hidden Window	Input Capture	File and Directory Discovery		Automated Collection	Standard Cryptographic Protocol		Defacement
		New Service	Process Injection	Modify Registry	Hooking	System Network Connections Discovery		Input Capture	Remote File Copy		
		Scheduled Task	Hooking	Obfuscated Files or Information		Query Registry					
		Hidden Files and Directories		File System Logical Offsets		System Network Configuration Discovery					
		Hooking		Masquerading		System Information Discovery					
				NTFS File Attributes		Network Share Discovery					
				Rootkit							
				Disabling Security Tools							
				Process Injection							
				Hidden Files and Directories							

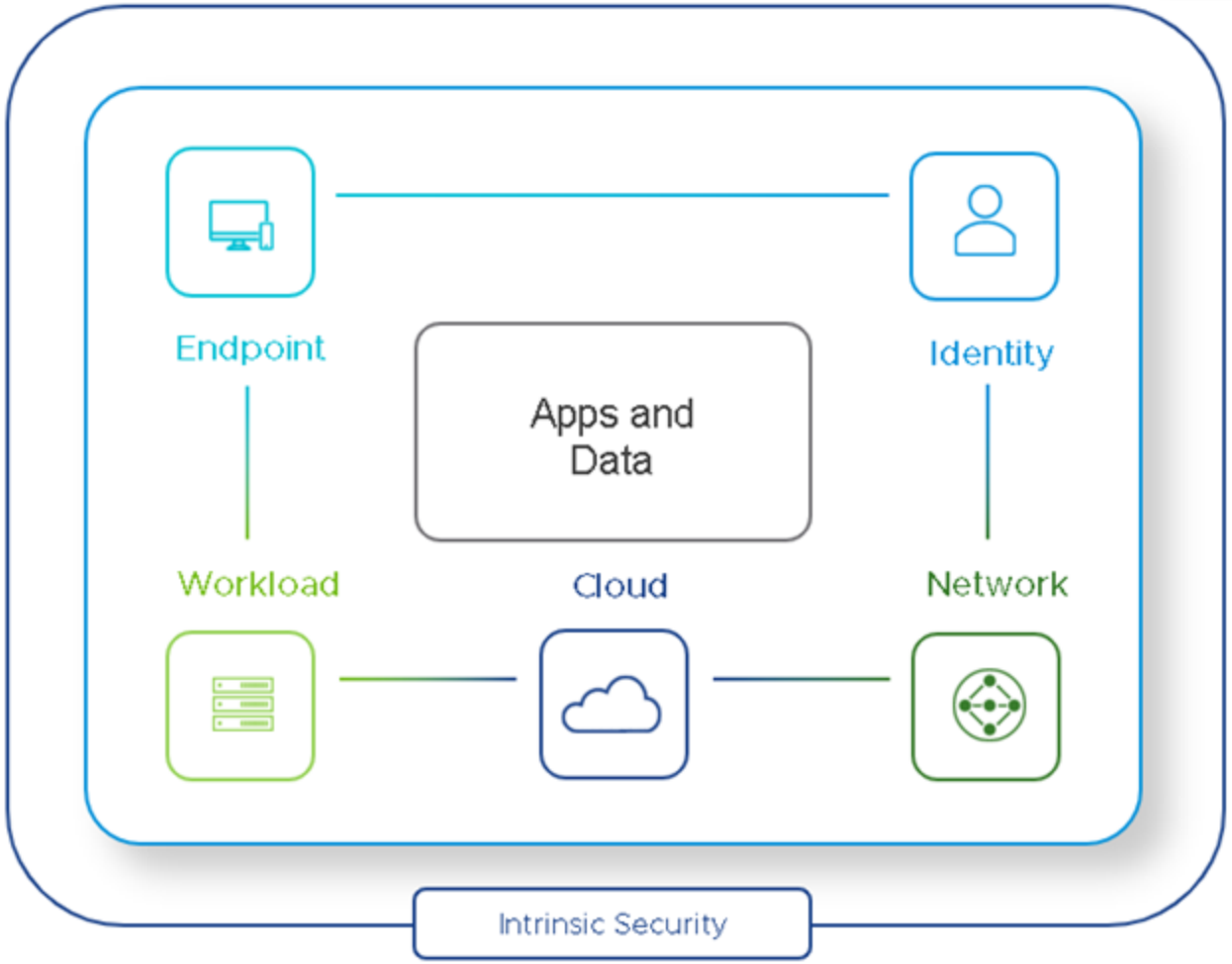
Wiper Behaviors



Defender Advice

- Thin out attack surface
- Get back to basics, backups and testing
- Continuous Recording via EDR
- Deploy Application Whitelisting
- PowerShell Logging
- Centralize Endpoint and Network Logs
- Focus on clustered behaviors
- Operate under the premise that attackers don’t leave

VMware Security Vision – Intrinsic Security



RSAConference2020

Thank you!

rmcelroy[at]vmware.com
@InfoSecRick

gfoss[at]vmware.com
@heinzarelli