The Circle Of Life: A Large-Scale Study of The IoT Malware Lifecycle

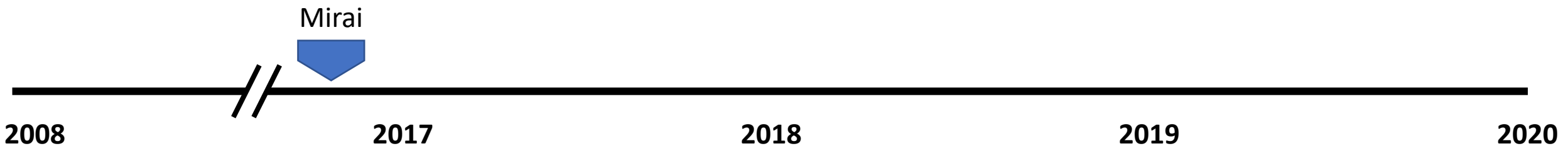
Omar Alrawi, Charles Lever, Kevin Valakuzhy, Ryan Court, Kevin Snow, Fabian Monrose, Manos Antonakakis

Georgia Tech

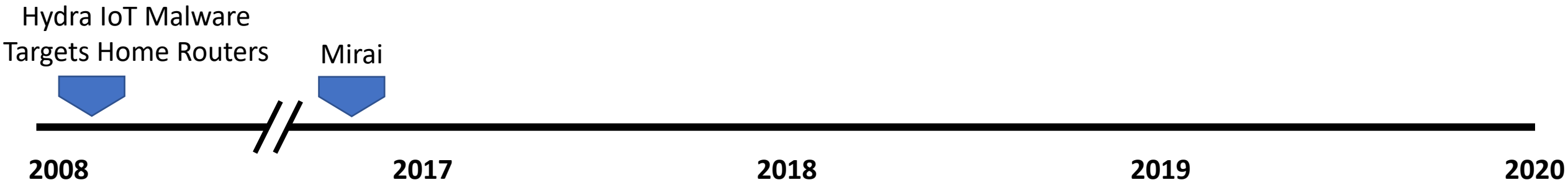
THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

ZEROPOINT

Motivation and Goals

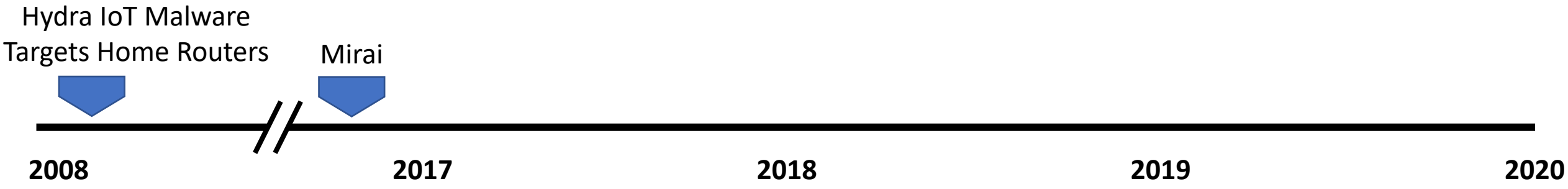


Motivation and Goals



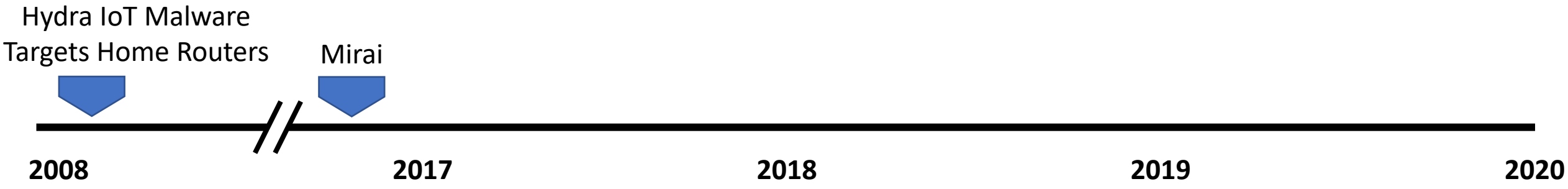
Motivation and Goals

1. **Is IoT malware any different?**



Motivation and Goals

1. **Is IoT malware any different?**
2. **Are we prepared for another Mirai-like attack?**



Motivation and Goals

1. **Is IoT malware any different?**
2. **Are we prepared for another Mirai-like attack?**

threatpost

Latest Mirai Variant Targets SonicWall, D-Link and IoT Devices

pindrop

NEW MIRAI VARIANT INFECTING HOME ROUTERS

DARKReading

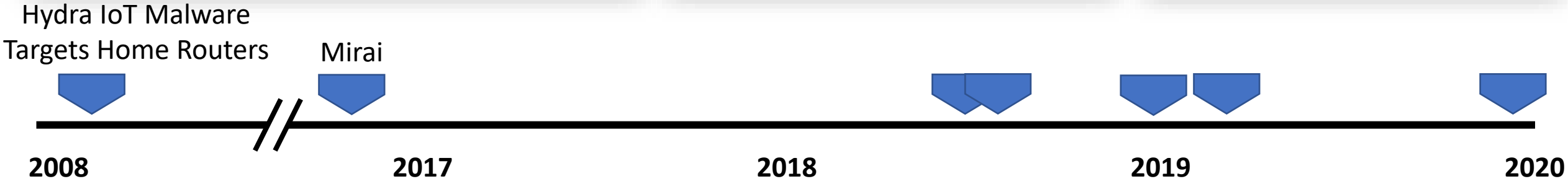
New Mirai Variant Surfaces with Exploits for 9 Vulnerabilities Products

imperva

New Mirai Variant Launches 54 Hour DDoS Attack against US College

avast

Seven new Mirai variants and the aspiring cybercriminal behind them



Prior Studies

Family Specific

Understanding the Mirai Botnet

Manos Antonakakis[◇] Tim April[‡] Michael Bailey[†] Matthew Bernhard[◁] Elie Bursztein[○]
Jaime Cochran[▷] Zakir Durumeric[◁] J. Alex Halderman[◁] Luca Invernizzi[○]
Michalis Kallitsis[§] Deepak Kumar[†] Chaz Lever[◇] Zane Ma[†*] Joshua Mason[†]
Damian Menscher[○] Chad Seaman[‡] Nick Sullivan[▷] Kurt Thomas[○] Yi Zhou[†]

[‡]*Akamai Technologies* [▷]*Cloudflare* [◇]*Georgia Institute of Technology* [○]*Google*

Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet

Stephen Herwig[1] Katura Harvey[1,2] George Hughey[1] Richard Roberts[1,2] Dave Levin[1]
[1]University of Maryland [2]Max Planck Institute for Software Systems (MPI-SWS)
{smherwig, katura}@cs.umd.edu, ghughey@terpmail.umd.edu, {ricro, dml}@cs.umd.edu

***Abstract*—The Internet of Things (IoT) introduces an unprece-**

While there have been in-depth studies into the kinds

Small Scale or Short Periods

IoT Malware Ecosystem in the Wild: A Glimpse into Analysis and Exposures

Jinchun Choi* jc.choi@knights.ucf.edu University of Central Florida
Afsah Anwar* afsahanwar@knights.ucf.edu University of Central Florida
Hisham Alasmary hisham@knights.ucf.edu University of Central Florida
Jeffrey Spaulding spauldi6@canisius.edu Canisius College
DaeHun Nyang nyang@inha.ac.kr Inha University
Aziz Mohaisen mohaisen@ucf.edu University of Central Florida

DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation

De Donno, Michele; Dragoni, Nicola; Giaretta, Alberto; Spognardi, Angelo

Published in:
Security and Communication Networks

Before Toasters Rise Up: A View Into the Emerging IoT Threat Landscape

Pierre-Antoine Vervier and Yun Shen

General Linux/Specific Phase

Understanding Linux Malware

Emanuele Cozzi Eurecom
Mariano Graziano Cisco Systems, Inc.
Yanick Fratantonio Eurecom
Davide Balzarotti Eurecom

Understanding Fileless Attacks on Linux-based IoT Devices with HoneyCloud

Fan Dang[1], Zhenhua Li[1*], Yunhao Liu[1,2], Ennan Zhai[3]
Qi Alfred Chen[4], Tianyin Xu[5], Yan Chen[6], Jingyu Yang[7]
[1]Tsinghua University [2]Michigan State University [3]Alibaba Group [4]University of California, Irvine
[5]University of Illinois Urbana-Champaign [6]Northwestern University [7]Tencent Anti-Virus Lab

ABSTRACT

have employed Linux (*e.g.*, OpenWrt and Raspbian) for its preva-
lence and programmability, and such a trend has been growing

Many Challenges to Study IoT Ecosystem

Representative Data

Data sources for the IoT malware must be representative. Require large collaboration.

Many Challenges to Study IoT Ecosystem

Representative Data

Data sources for the IoT malware must be representative. Require large collaboration.

Large-Scale Dataset

Large-scale data provides a better perspective on malware in-the-wild

Many Challenges to Study IoT Ecosystem

Representative Data

Data sources for the IoT malware must be representative. Require large collaboration.

Large-Scale Dataset

Large-scale data provides a better perspective on malware in-the-wild

Lack of Analysis Tools

IoT malware targets many system arch., Including ARM, MIPS, PPC, and others. Tools need to be tailored.

Many Challenges to Study IoT Ecosystem

Representative Data

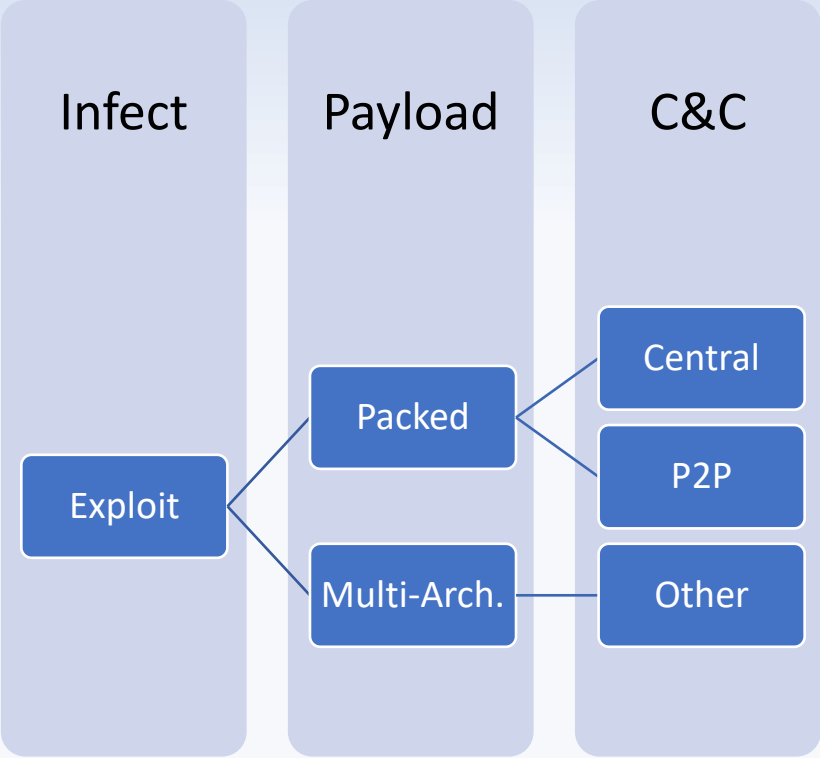
Data sources for the IoT malware must be representative. Require large collaboration.

Large-Scale Dataset

Large-scale data provides a better perspective on malware in-the-wild

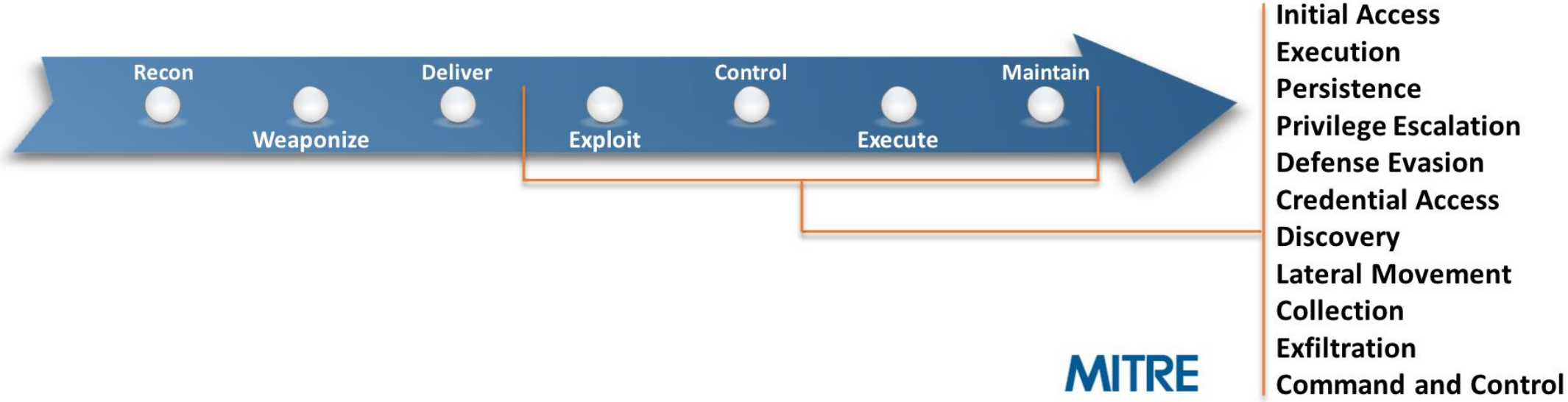
Lack of Analysis Tools

IoT malware targets many system arch., Including ARM, MIPS, PPC, and others. Tools need to be tailored.



Many Phases and Different Tactics

Key Idea: Study *IoT Malware* Through The Lens of *Traditional Malware*



Key Idea: Study *IoT Malware* Through The Lens of *Traditional Malware*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files		Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control				Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking				Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking				Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation				Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection				Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness				Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking				Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection				SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon				Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service				Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception				Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification				Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors							Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection							Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task							Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness							Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid							
	Signed Script Proxy Execution	Launch Agent								
	Source									
	Space after Filename									

MITRE

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

Key Idea: Study *IoT Malware* Through The Lens of *Traditional Malware*

Infection **Payload** **Persistence** **Capabilities** **C&C**

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files		Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CM			Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Co			Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Co			Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Co			Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Co			Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	Co			Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Di			Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Di			SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Di			Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Di			Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Di			Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Di			Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	Di						Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	Di						Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Di						Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Di						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Di						
	Signed Script Proxy Execution	Launch Agent		Di						
	Source			Di						
	Space after Filename			Di						
				Exp						
				Ext						
				File						
				File System Logical Offsets		System Information Discovery				
				Gatekeeper Bypass	Securityd Memory	System Network Configuration Discovery				
				Hidden Files and Directories	Two-Factor Authentication Interception	System Network Connections Discovery				
				Hidden Users		System Owner/User Discovery				
				Hidden Window		System Service Discovery				
				HISTCONTROL						
				Image File Execution Options Injection						

MITRE

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

Key Idea: Study *IoT Malware* Through The Lens of *Traditional Malware*

Infection **Payload** **Persistence** **Capabilities** **C&C**

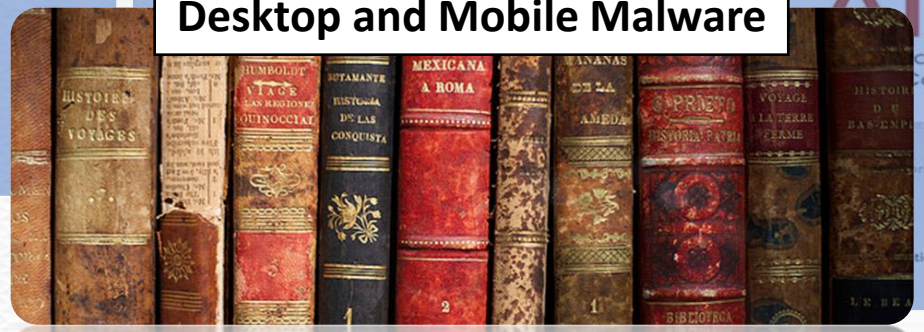
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files		Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control				Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking				Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking				Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions					Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts		Change Default File Association					Remote Services	Input Capture		Multi-hop Proxy
							Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
							Shared Webroot	Screen Capture		Multiband Communication
							SSH Hijacking	Video Capture		Multilayer Encryption
							Taint Shared Content			Port Knocking
							Third-party Software			Remote Access Tools
							Windows Admin Shares			Remote File Copy
							Windows Remote Management			Standard Application Layer Protocol
										Standard Cryptographic Protocol
										Standard Non-Application Layer Protocol
										Uncommonly Used Port
										Web Service

MITRE

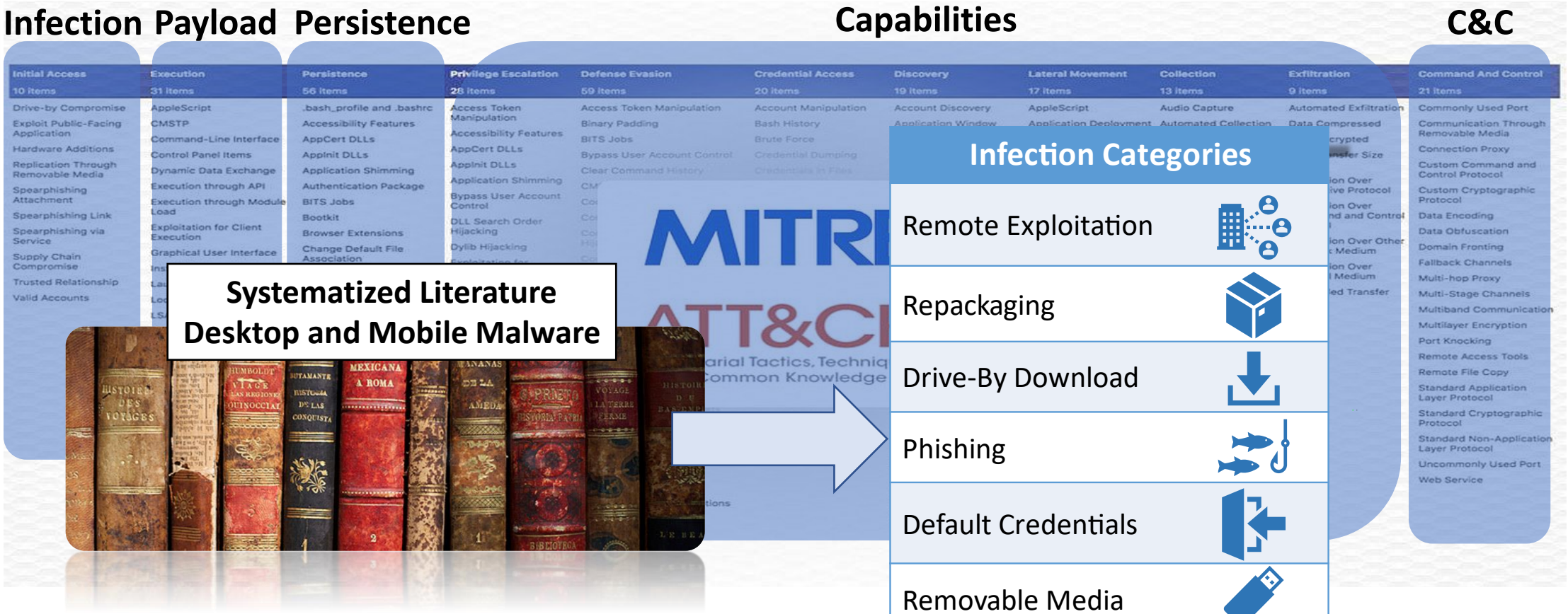
ATT&CK™

arial Tactics, Techniques
Common Knowledge

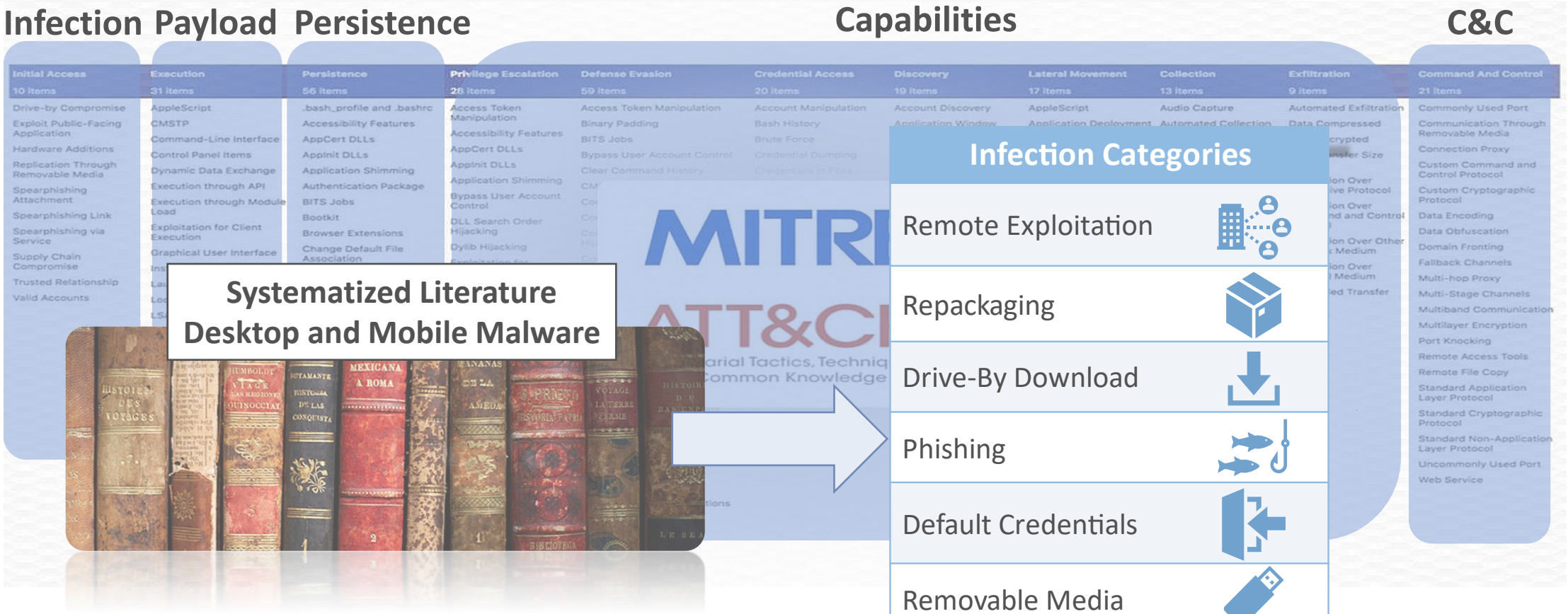
Systematized Literature
Desktop and Mobile Malware



Key Idea: Study *IoT Malware* Through The Lens of *Traditional Malware*



Key Idea: Study *IoT Malware* Through The Lens of *Traditional Malware*



Empirical Approach

Data Sources

VirusTotal

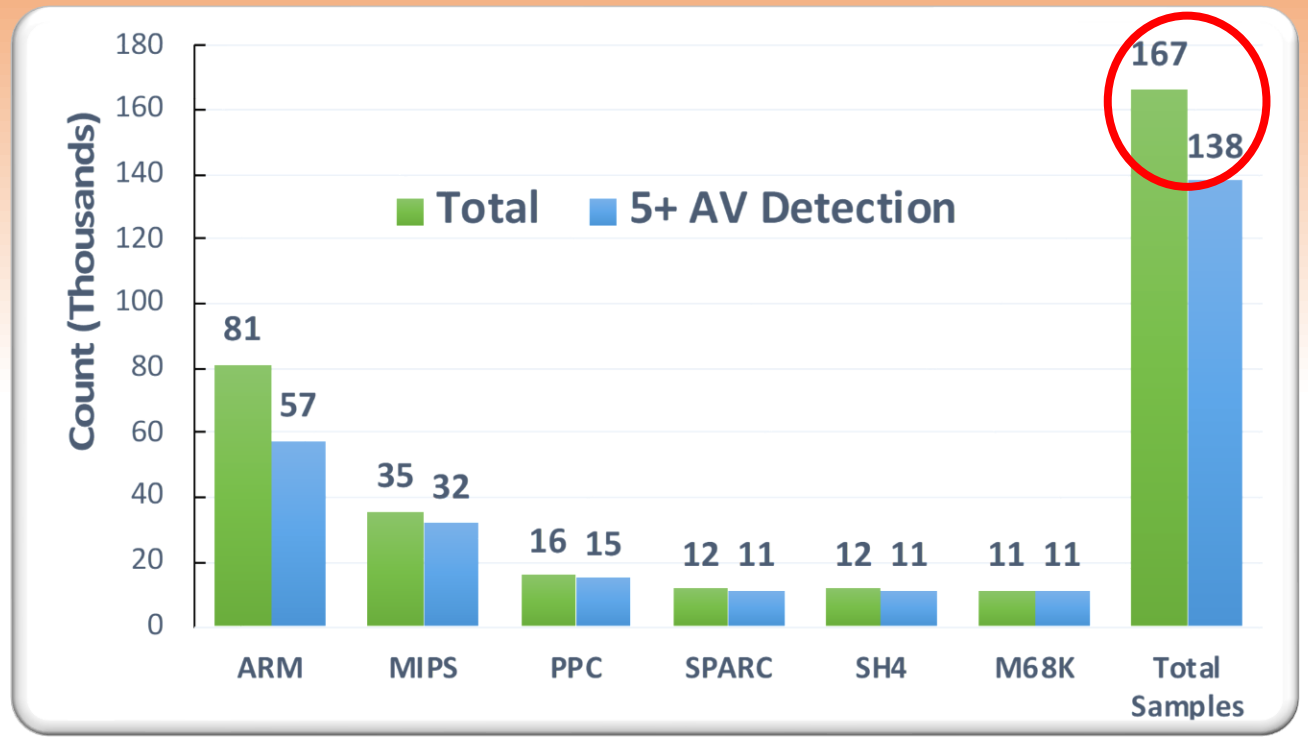
BAD PACKETS

Active-DNS

Passive-DNS

Tranco: Top Sites

Empirical Approach



Data Sources

VirusTotal

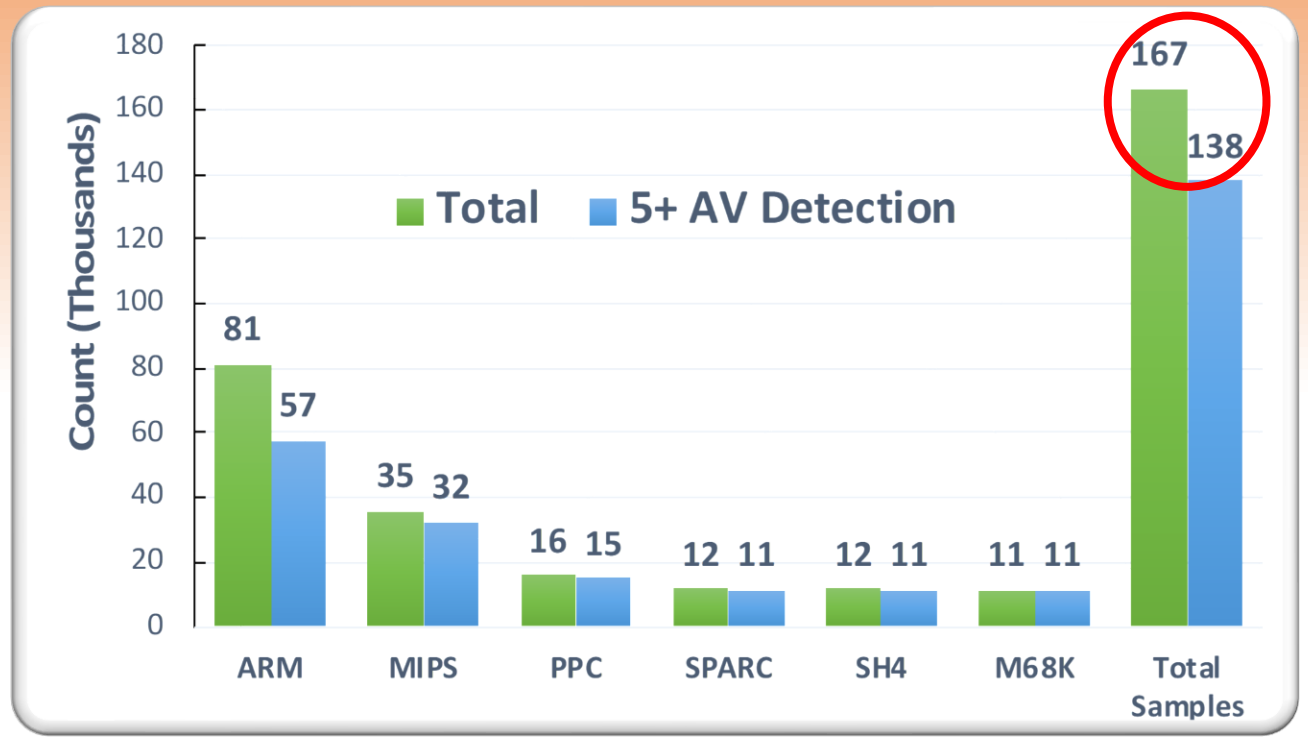
BAD PACKETS

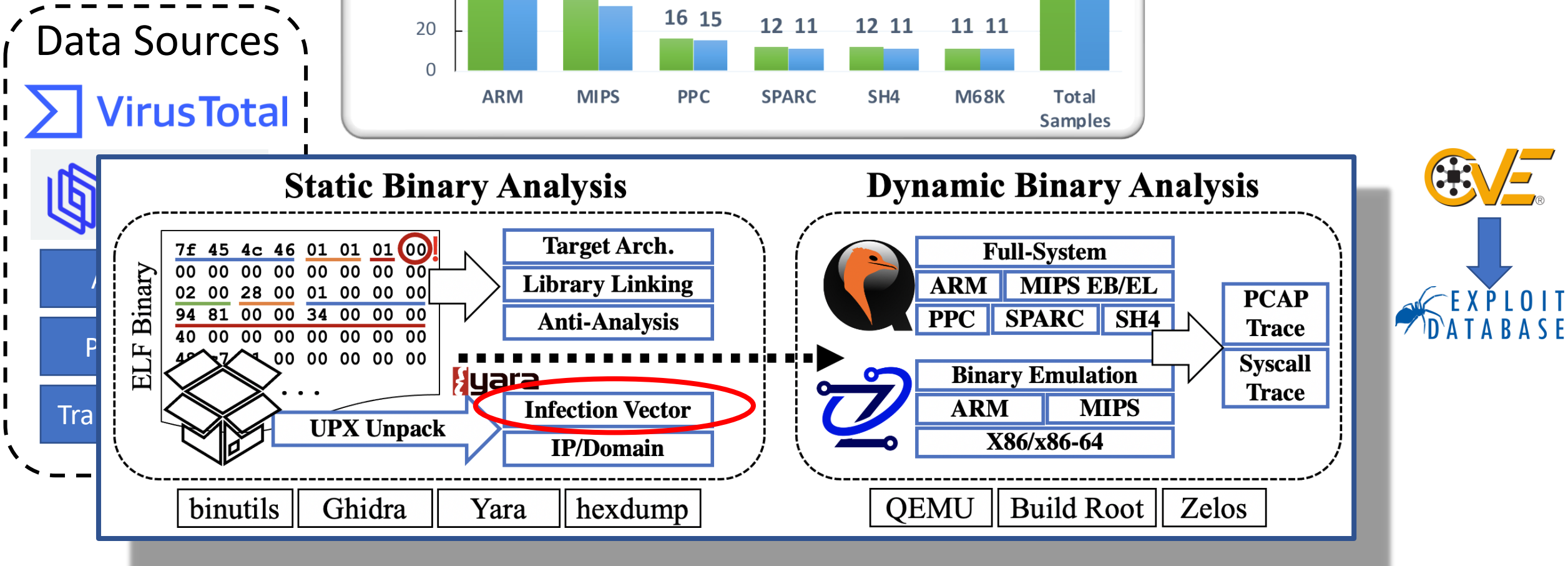
Active-DNS

Passive-DNS

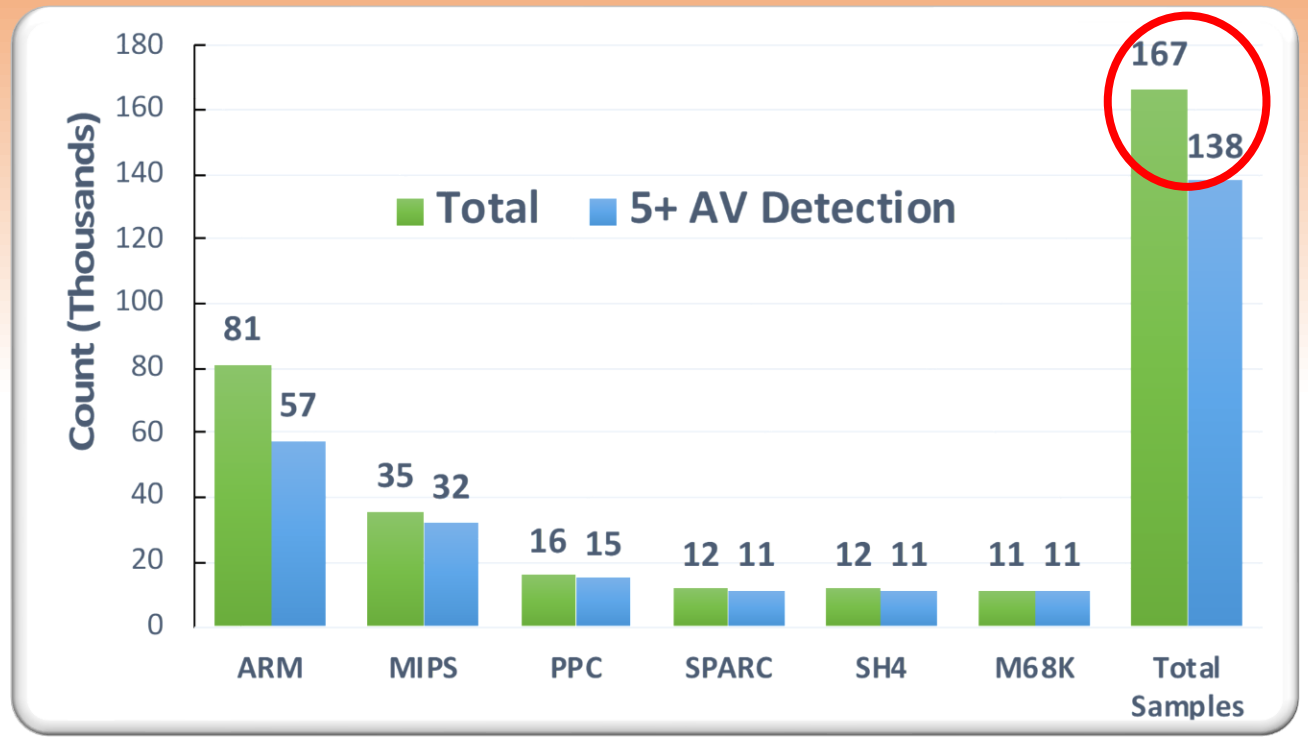
Tranco: Top Sites

Empirical Approach



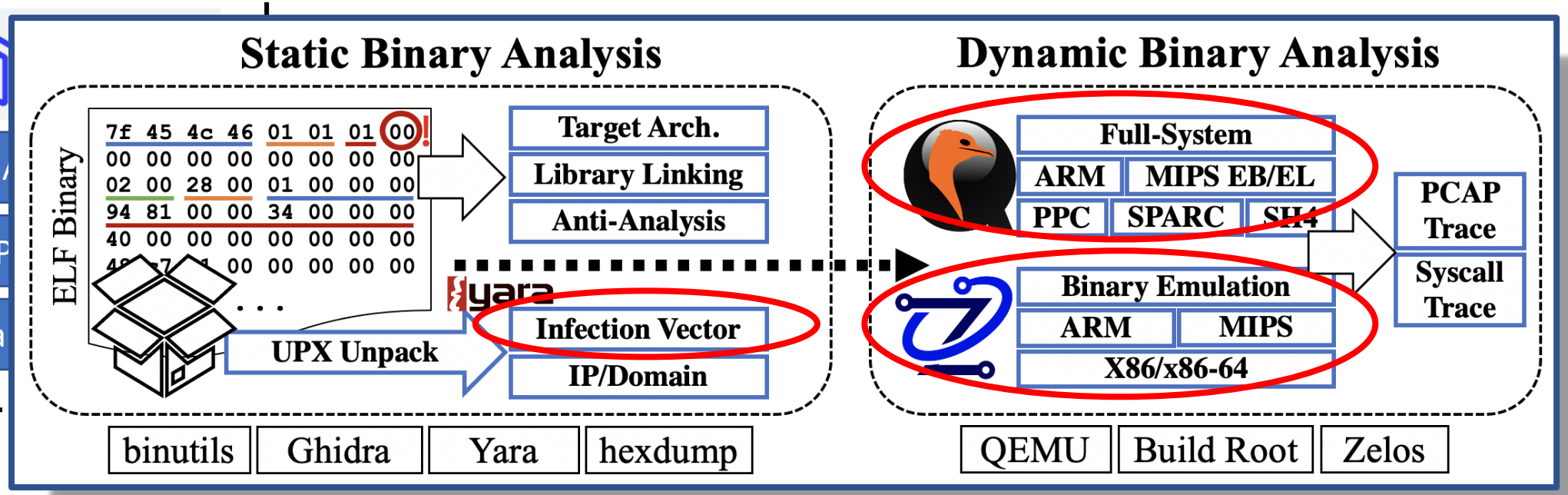


Empirical Approach



Data Sources

VirusTotal



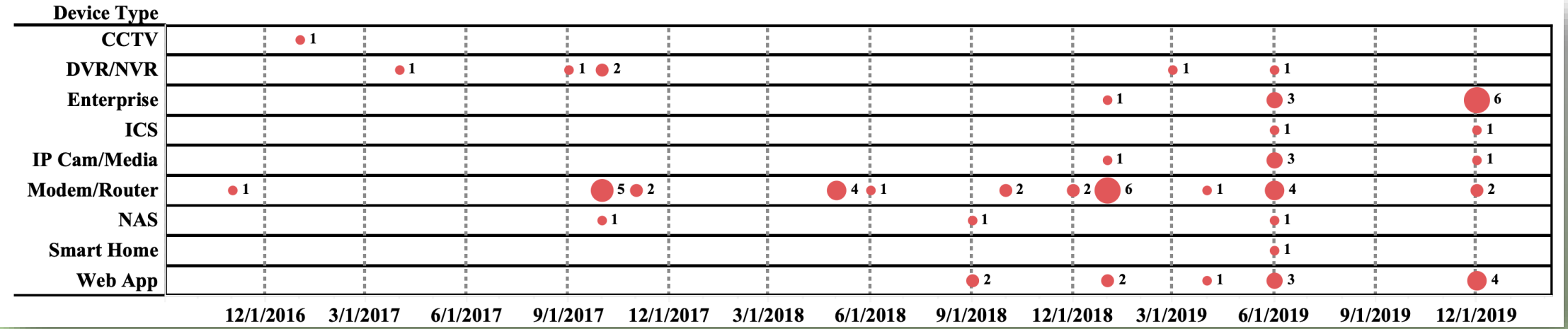
CVE

EXPLOIT DATABASE

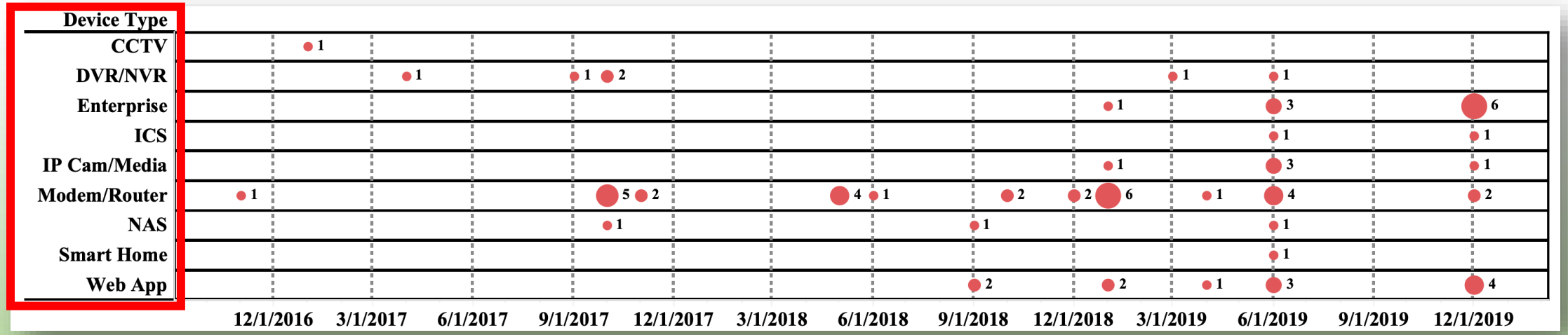
BuildRoot Making Embedded Linux Easy

ZEROPOINT

Infection Analysis

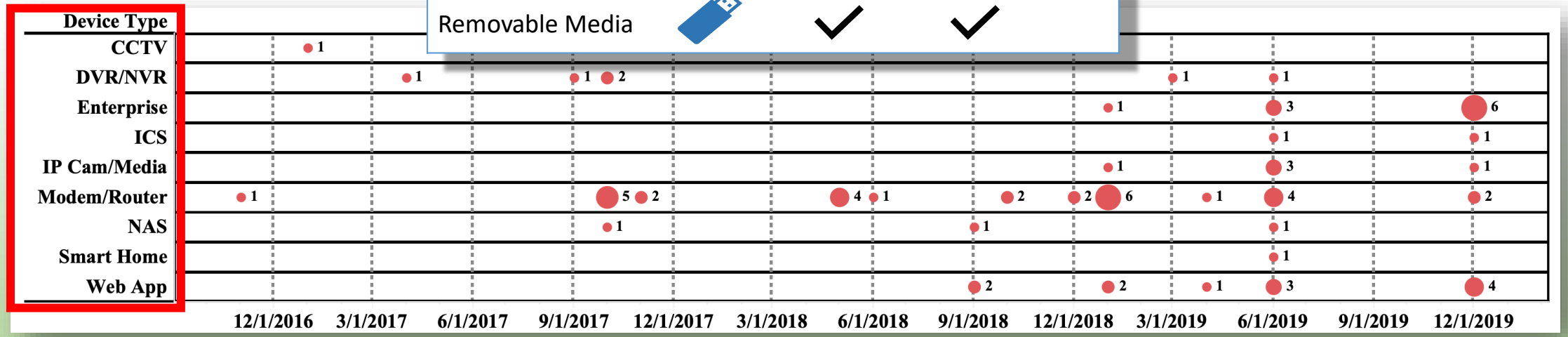


Infection Analysis



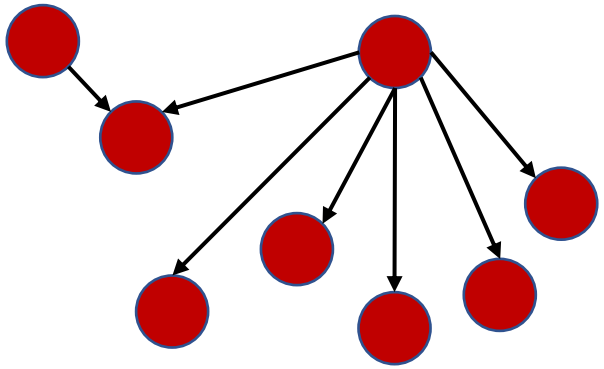
Infection Analysis

Infection Categories	Desktop	Mobile	IoT
Remote Exploitation	✓		✓
Repackaging	✓	✓	
Drive-By Download	✓	✓	
Phishing	✓	✓	
Default Credentials	✓		✓
Removable Media	✓	✓	

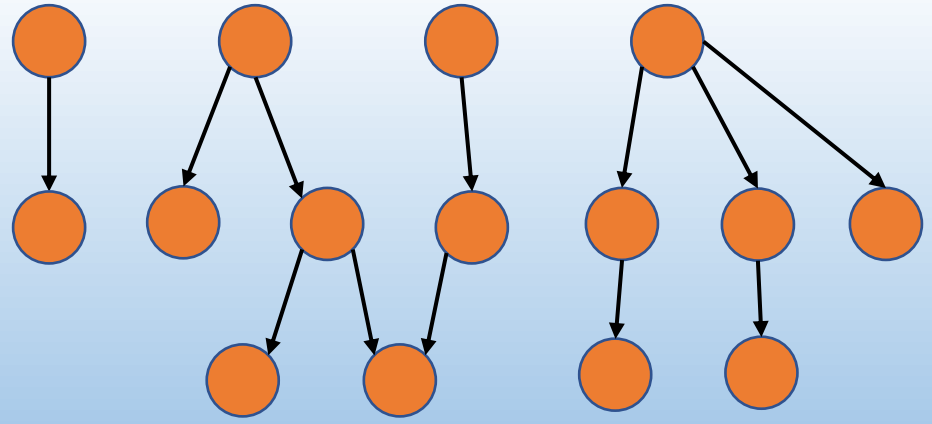


Payload Analysis

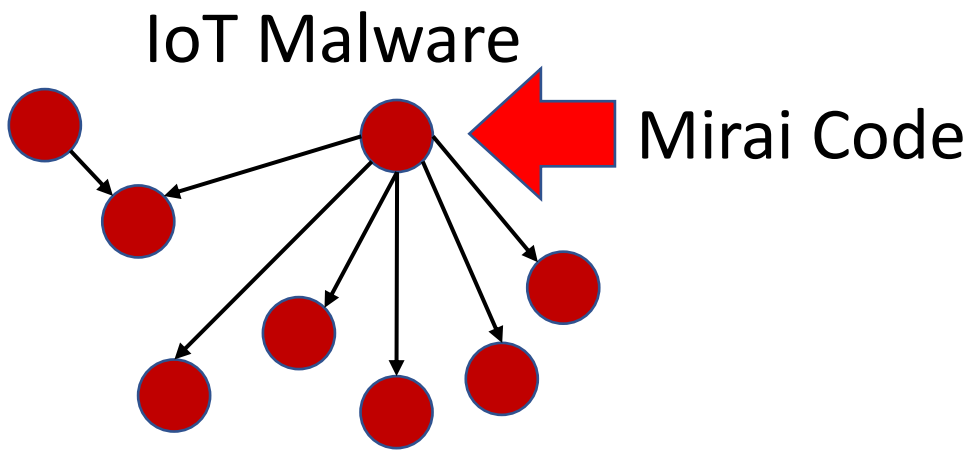
IoT Malware

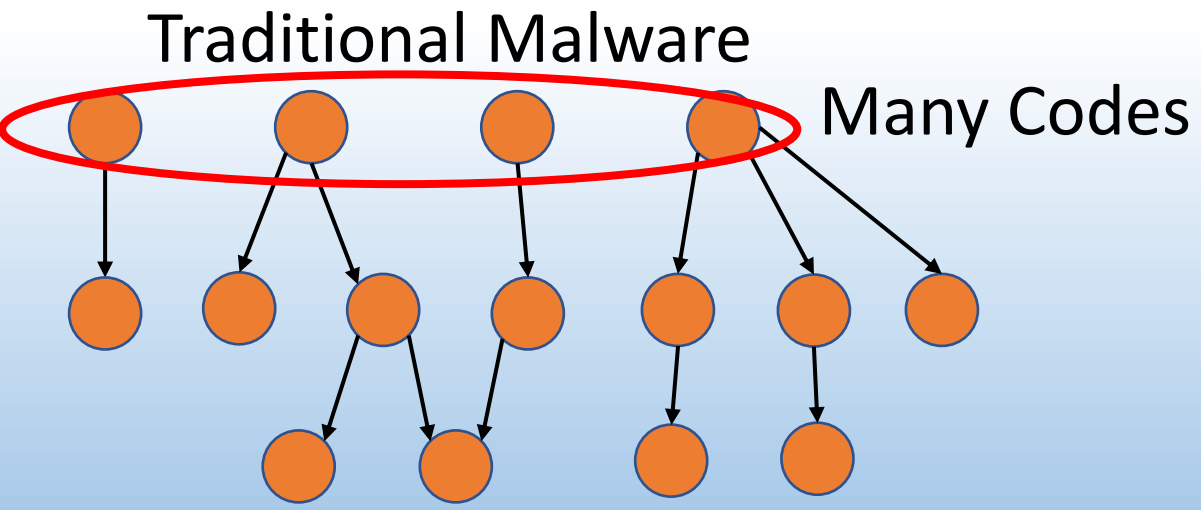


Traditional Malware



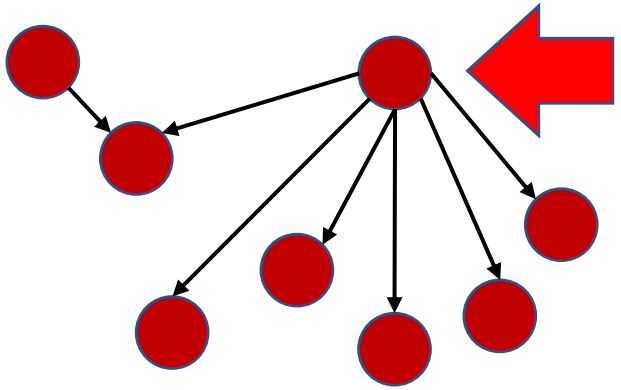
Payload Analysis





Payload Analysis

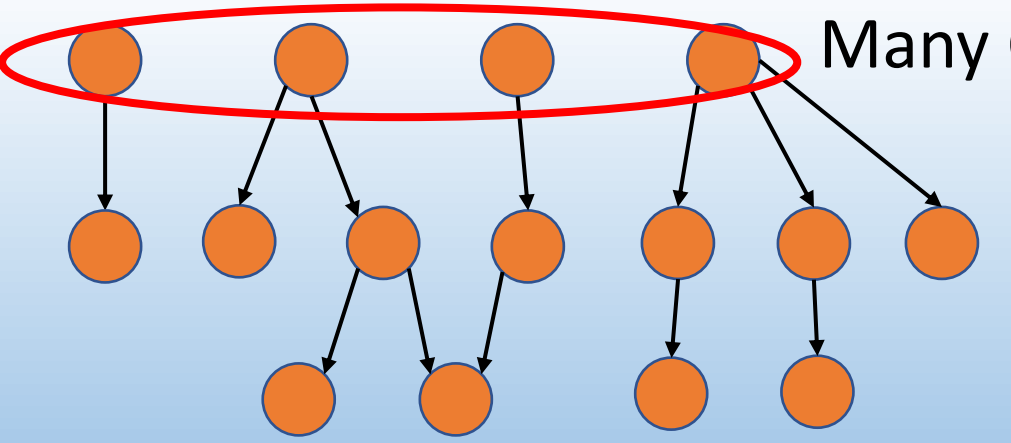
IoT Malware



Mirai Code

Polymorphic Malware

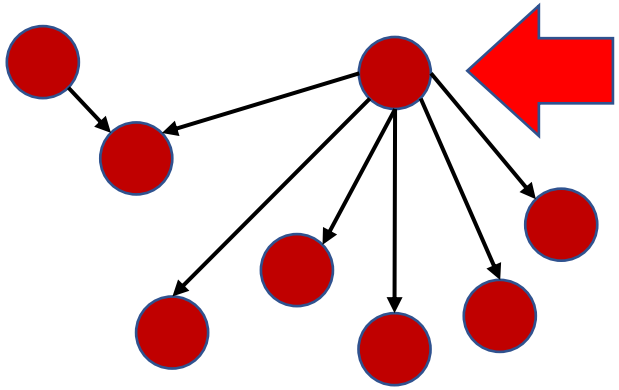
Traditional Malware



Many Codes

Payload Analysis

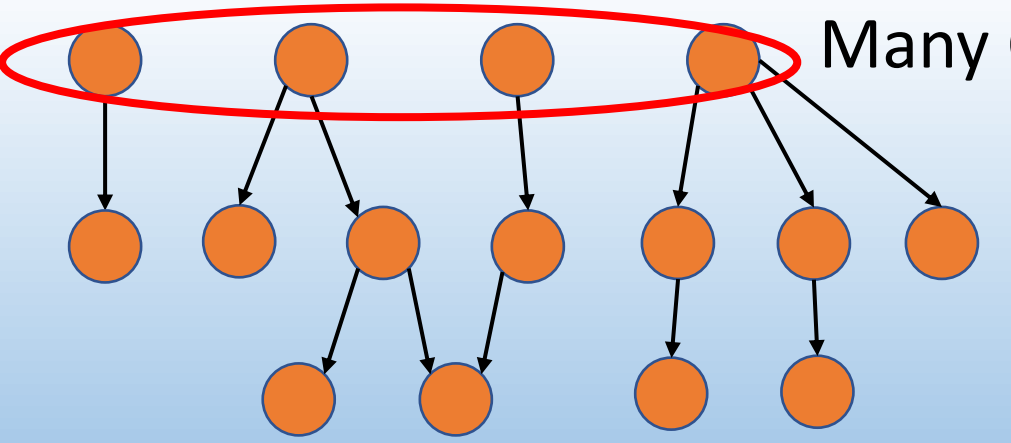
IoT Malware



Mirai Code

Polymorphic Malware

Traditional Malware



Many Codes

Payload Categories	Desktop	Mobile	IoT
Packing	✓	✓	✓
Environment Keying	✓	✓	✓
Scripting	✓		✓
Cross-arch./plat.	✓	✓	✓

Persistence and Capability Analysis

Persistence

Read-Only File Systems

Capabilities

Persistence and Capability Analysis

Persistence

Read-Only File Systems

Vendor-Specific Tools

Capabilities

Persistence and Capability Analysis

Persistence

Read-Only File Systems

Vendor-Specific Tools

Remount File Systems

Capabilities

Persistence and Capability Analysis

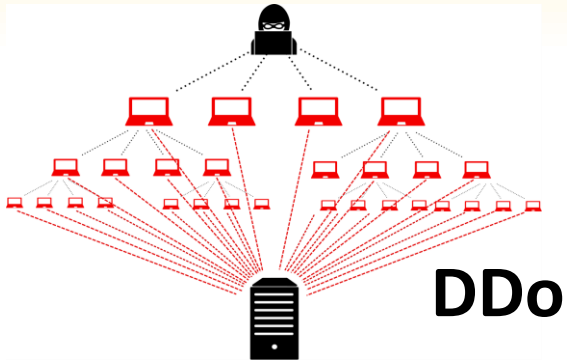
Persistence

Read-Only File Systems

Vendor-Specific Tools

Remount File Systems

Capabilities



DDoS

Persistence and Capability Analysis

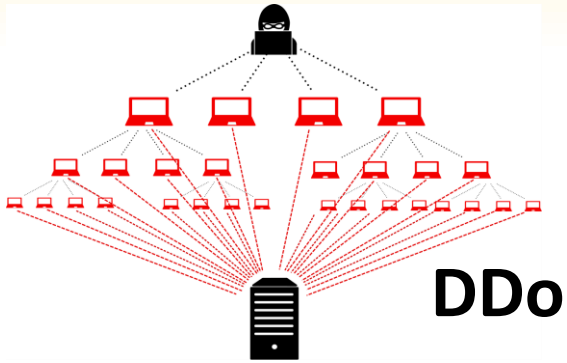
Persistence

Read-Only File Systems

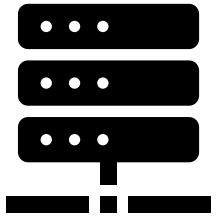
Vendor-Specific Tools

Remount File Systems

Capabilities



DDoS



Proxy Servers

Persistence and Capability Analysis

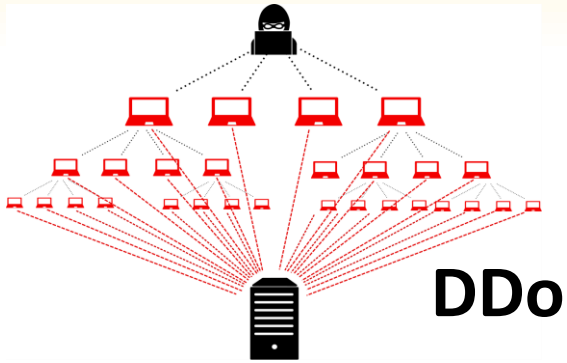
Persistence

Read-Only File Systems

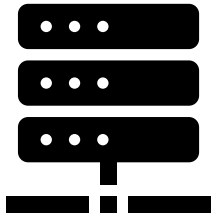
Vendor-Specific Tools

Remount File Systems

Capabilities



DDoS



Proxy Servers

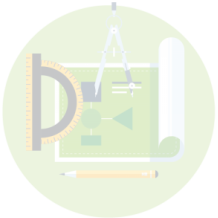
Crypto Mining

Persistence and Capability Analysis

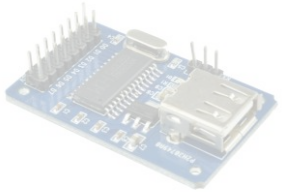
Persistence

Capabilities

Read-Only File Sy



Vendor-Specific T



Remount File Sy

Persistence Categories	Desktop	Mobile	IoT
Firmware	✓		✓
Kernel Space	✓	✓	+
User Space	✓	✓	+
Capability Categories	**Desktop**	**Mobile**	**IoT**
Escalation	✓	✓	✓
Evasion	✓	✓	✓
Theft	✓	✓	✓
Scanning	✓		✓
DDoS	✓		✓
Destruction	✓	✓	✓
Resource Abuse	✓	✓	✓

DDoS

Proxy Servers

Crypto Mining

C&C Communication Analysis

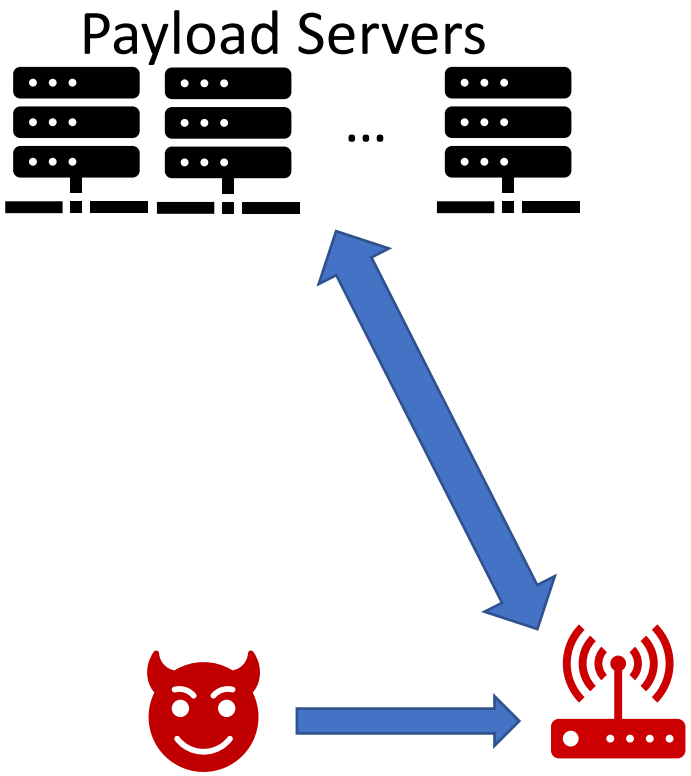
Centralized

C&C Communication Analysis

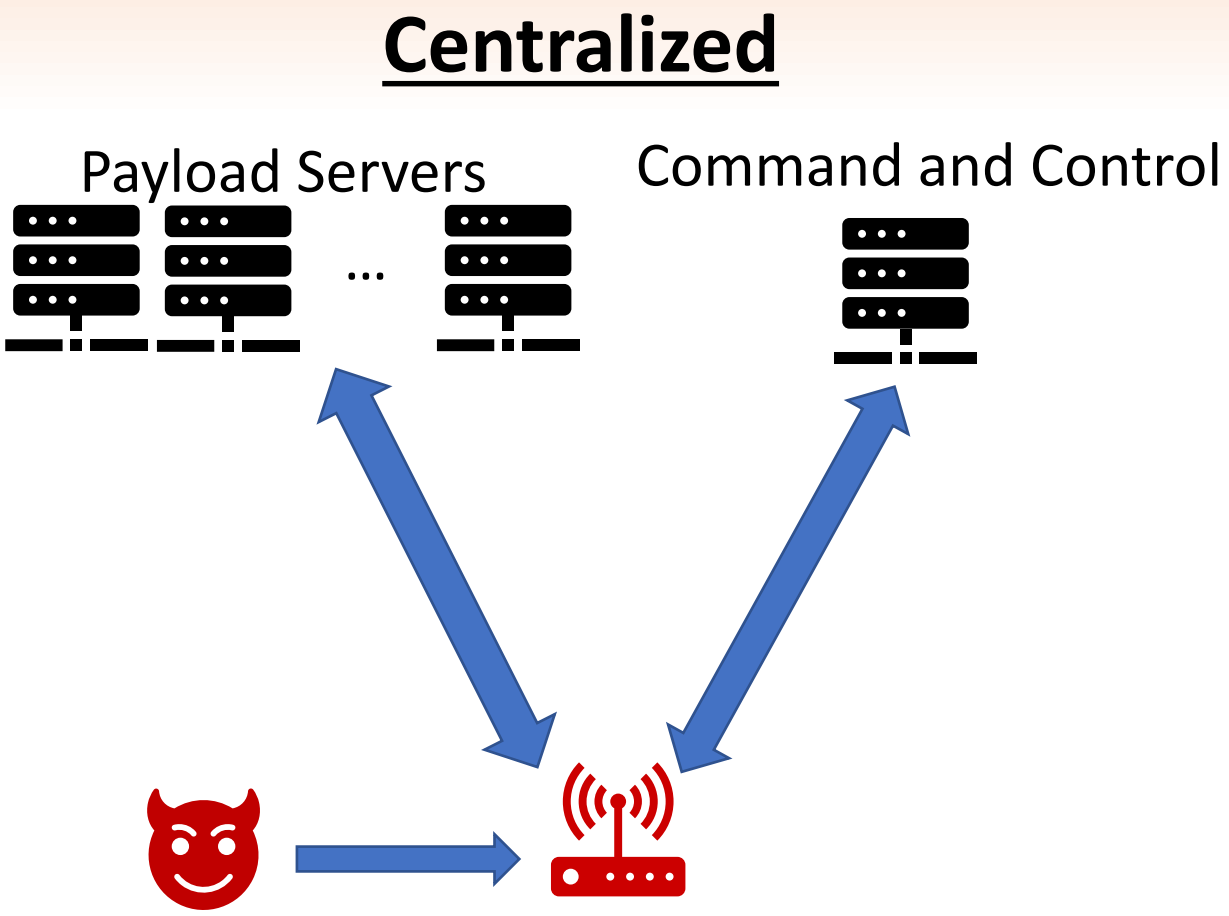
Centralized

C&C Communication Analysis

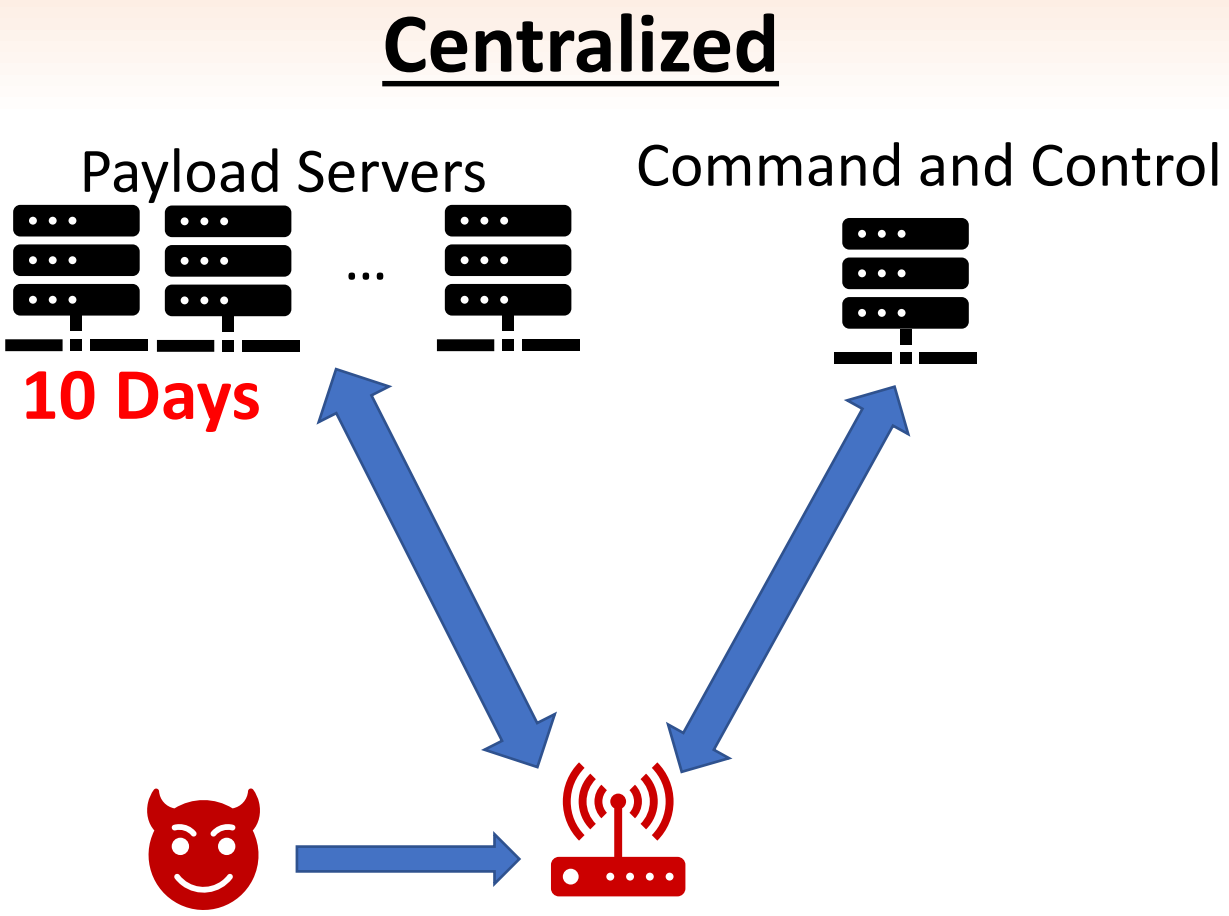
Centralized



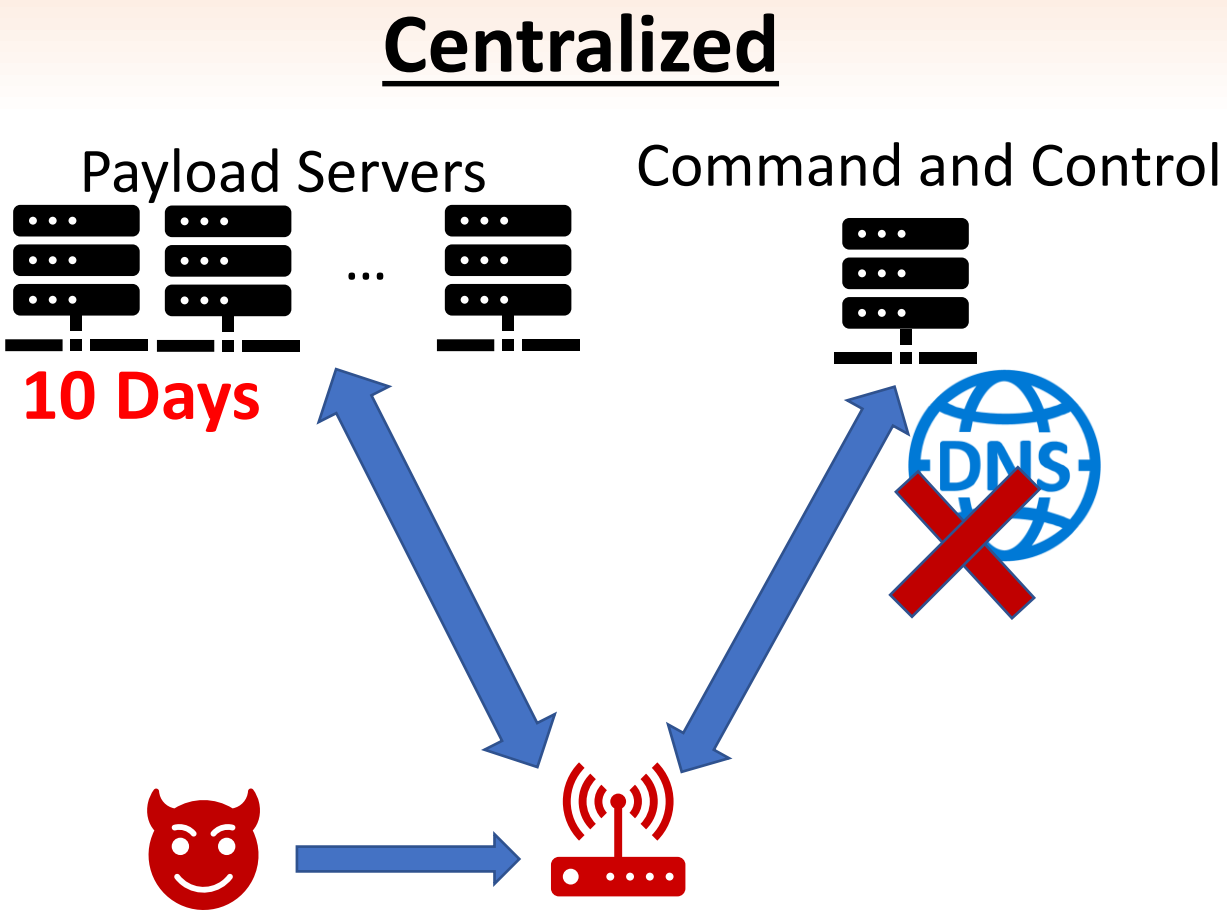
C&C Communication Analysis



C&C Communication Analysis

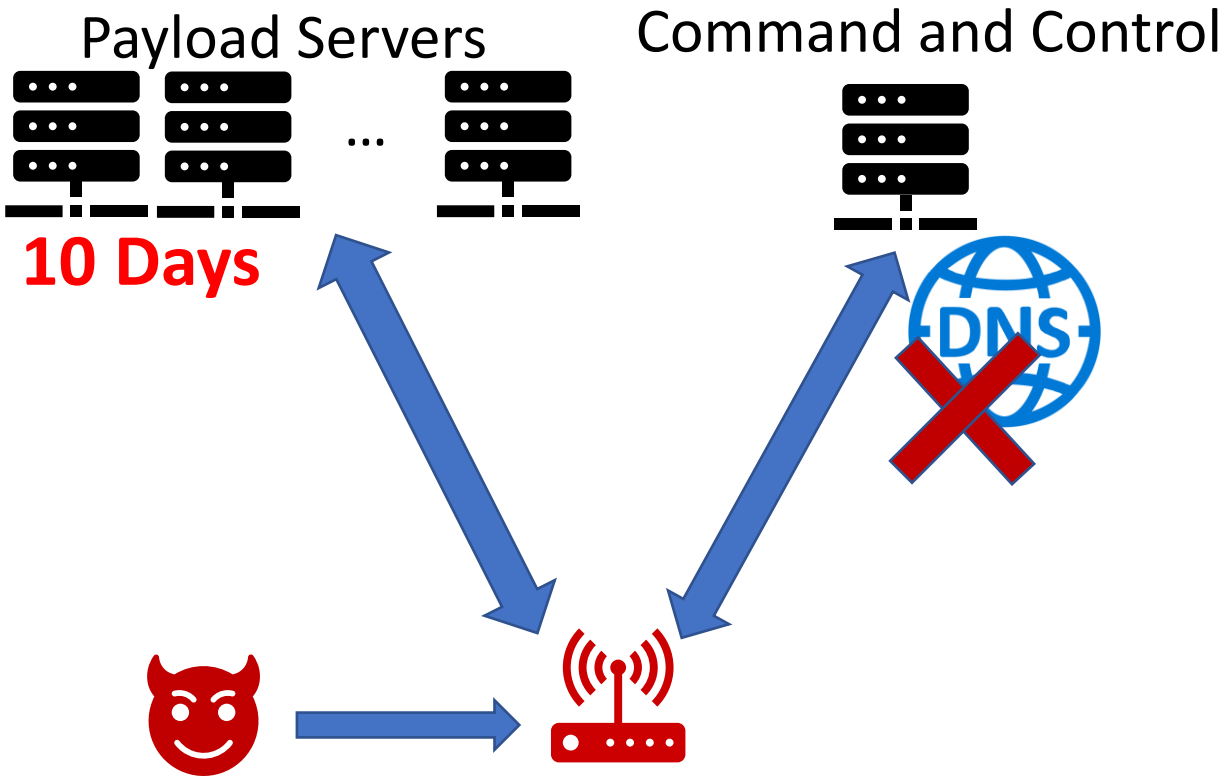


C&C Communication Analysis

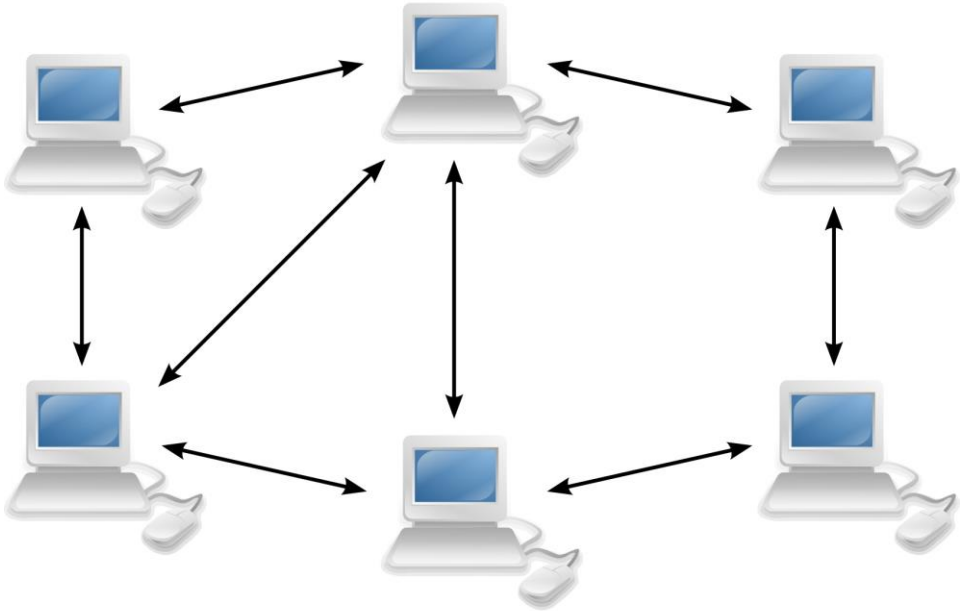


C&C Communication Analysis

Centralized



Peer-2-Peer



C&C Communication Analysis

Centralized **Peer-2-Peer**

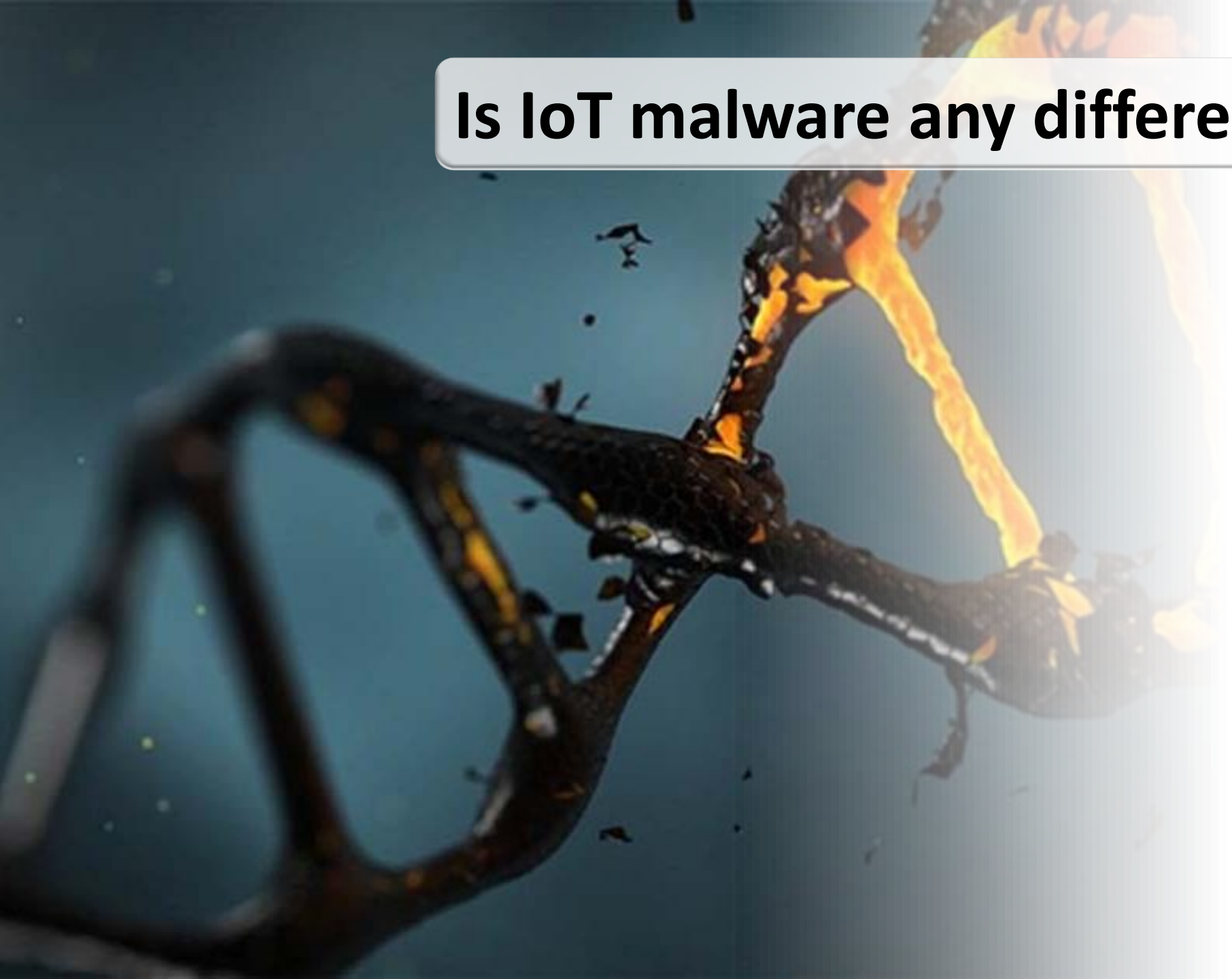
Payload Servers

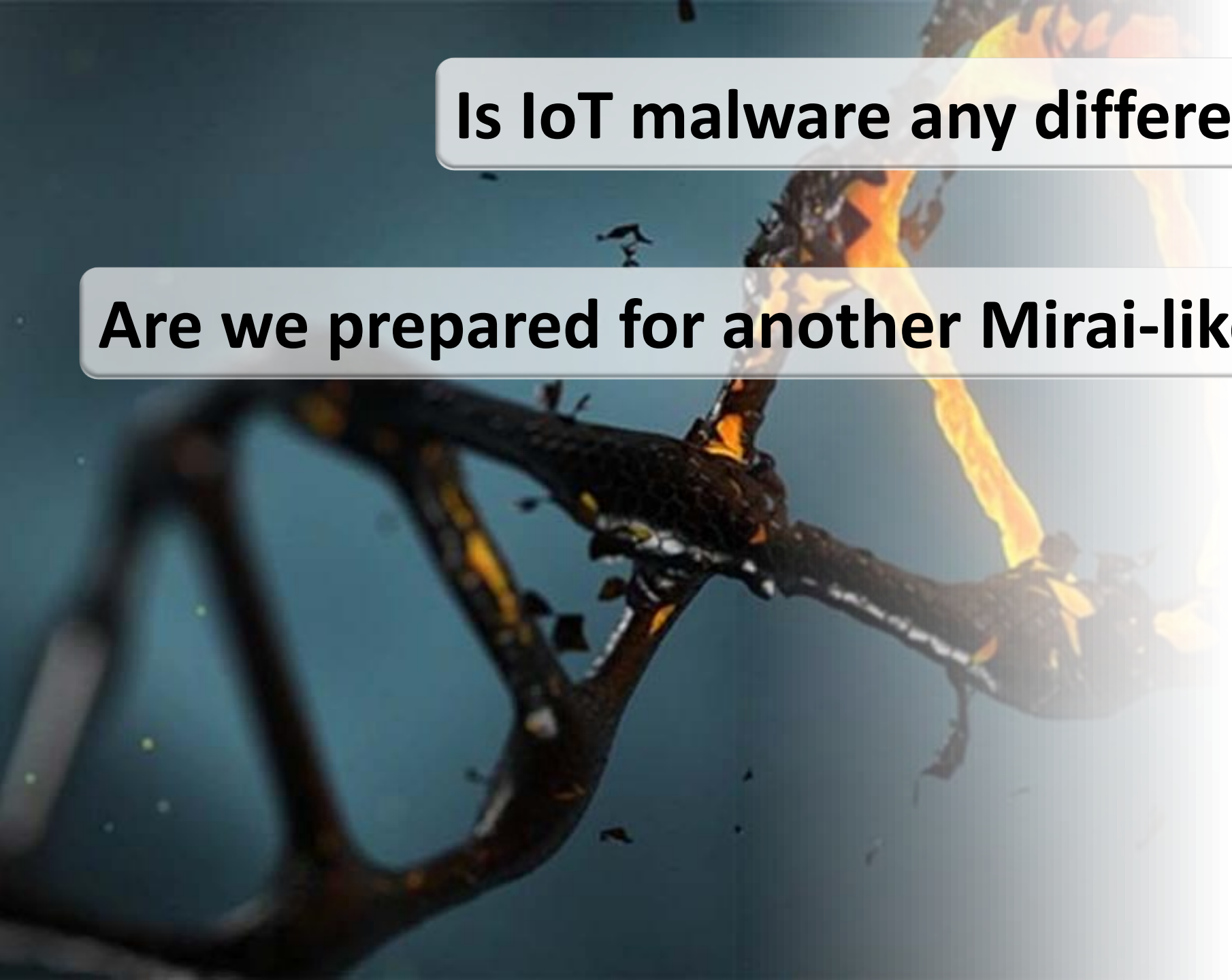
Command and Control

10 Days

C&C Categories	Desktop	Mobile	IoT
Peer-2-Peer	✓		✓
Centralized	✓	✓	✓
Email/SMS	✓	✓	

Is IoT malware any different?





Is IoT malware any different?

Are we prepared for another Mirai-like attack?

Is IoT malware any different?

Are we prepared for another Mirai-like attack?

THE WHITE HOUSE

(s) The Secretary of Co[illegible]e

Director of NIST, in coordination with representatives of other agencies as the Director of NIST deems appropriate, shall initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs.

Is IoT malware any different?

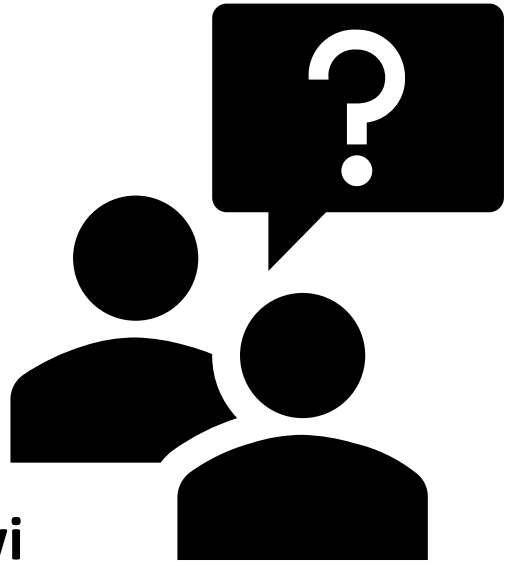
Are we prepared for another Mirai-like attack?

THE WHITE HOUSE

(s) The Secretary of Co[illegible]e Director of NIST, in coordination with representatives of other agencies as the Director of NIST deems appropriate, shall initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs.

Mirai Infected Devices		Hajime Infected Devices	
Country	Count	Country	Count
Brazil	15.0%	Iran	29.0%
Colombia	14.0%	Russia	9.6%
Vietnam	12.5%	Italy	9.3%
China	6.5%	China	6.2%
S. Korea	6.0%	Turkey	5.6%
Russia	4.7%	India	5.0%
Turkey	4.2%	Brazil	5.0%
India	4.1%	Pakistan	4.6%
Taiwan	3.5%	Australia	3.9%
Argentina	2.2%	Thailand	3.4%

Questions



Omar Alrawi

alrawi@gatech.edu

https://alrawi.io

BadThings

https://BadThings.info

YourThings Scorecards

https://YourThings.info

contact@badthings.info