COSC 366
Intro to Cybersecurity

Dr. Suya

Fall 2024

Today's Class

- Malware 101
- Classic malware
- Emerging malware threats

What Is Malware?

- Malicious software: software that intentionally designed or deployed to have effects contrary to the best interests of users, including potential damage related to resources, devices, or other systems
- Damage may include
  - data
  - software
  - hardware
  - compromise of privacy
  - loss of reputation

Which CIA Goals Can Malware Violate?

- All of them

How Does Malware Get on Computers?

- Most common today: via websites
  - links in phishing emails
  - links on social media
  - search engine results
  - web page ads redirecting traffic
  - …

What Makes Malware Hard to Detect?

- Malware depends on context, not functionality, e.g., SSH
  - Can be tricky to differentiate between malicious and legitimate examples
  - Legit usage of SSH enables secure communication over network
  - Attacker can hijack the system and obtains unauthorized access to systems with (same) SSH
- Personal viewpoints may differ
  - Is a benign program that displays revenue-generating ads malicious?
  - for a user that plays free game, maybe not; for others, it is

Malware is specifically designed to evade detection or reverse-engineering

The Classic Malware

- Virus
  - a program that can infect (e.g., attach to) other programs or files by modifying them, and to potentially include an evolved copy of itself
- Worm
  - a standalone program that can replicate itself and send copies from computer to computer across network connections

Virus vs. Worm

- They both replicate: e.g., to infect different parts of the system
- They both propagate: infect as many systems as possible
- They both can contain trigger conditions

- Virus usually needs a host program; worm is independent or standalone (self-contained)
- Virus usually propagates with user interaction; worm propagates automatically and continuously via network
- Virus tends to abuse software features; worm usually exploits software vulnerabilities (e.g., bug in common Windows OS)

Virus vs. Worm

Computer virus	Computer worm

loop
  remain_dormant_until_host_runs();
  propagate_with_user_help();
  if trigger_condition_true() then
  run_payload();
endloop;
	loop
	  propagate_over_network();
	  if trigger_condition_true() then
	  run_payload();
	endloop

Basic Virus Structure

```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

Code Red Worm (MSFT Internet Information Service)

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0
```

N: Overflow the buffer

NOP

shellcode

Exploits the buffer overflow vulnerability in software

Worm uses the HTTP 1.0 protocol to send the request.

The Emerging Malware

- Ransomware

  - malware from cryptovirology that threatens to publish the victim's sensitive data or perpetually block access to it unless a ransom is paid

  - crypto ransomware: blocks access by encrypting files

  - non-crypto ransomware: blocks access by standard access control means; or threatens to publish data/erase files/reformat disks/etc.

  - unique in its motive: to extort users

WannaCry Ransomware

- Most affected countries: Russia, Ukraine, India, Taiwan
- Most affected organization: National Health Services hospitals in England and Scotland

WannaCry Ransomware

The Emerging Trio

- Botnet
  - a number of Internet-connected devices, each of which is running one or more bots
  - a bot is a device that has been compromised by malware and is used to launch attacks under remote control
  - popular attacks: DDoS, spam campaigns
  - unique in its use: booter service, you pay to get the service without knowing the technical details
    - DDoS for hire, attack infrastructure as a service

Mirai Botnet for Rent (target IoT devices)

Rent from Biggest Mirai Botnet (400k+ devices)
We use 0day exploits to get devices - not only telnet and ssh scanner.
Anti ddos mitigation techniques for tcp/udp.
Limited spots - Minimum 2 week spot.
Flexible plans and limits.
Free short test attacks, if we have time to show.

BestBuy provided an example: "price for 50,000 bots with attack duration of 3600 secs (1 hour) and 5-10 minute cooldown time is approx 3-4k per 2 weeks." As you can see, this is no cheap service.

The Emerging Trio

- Phishing
  - a social engineering attack where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information or deploying malware on the victim's infrastructure
  - unique in its tactics for delivering malware

Crypto Ransomware

[Mehnaz et al., RWGuard: A Real-Time Detection System Against Cryptographic Ransomware, (RAID'18)]

Crypto Ransomware

- Challenges addressed
  - existing detections fail to provide early warning
  - existing detections have high false positives

Crypto Ransomware

- RWGuard
- focuses on solving the most important problem on hand: providing early warning
- solution: deploy decoy files and normal process will not modify these files
- limitation: insider attacker who knows the deployment of decoy files

Crypto Ransomware

- RWGuard
  - the rapid encryption property of ransomware (maximize damage, minimize risk of detection)
  - solution: process monitor based on the running processes' I/O Request Packets (IRPs)
  - limitation: some ransomware like Crytolocker encrypts slowly

Crypto Ransomware

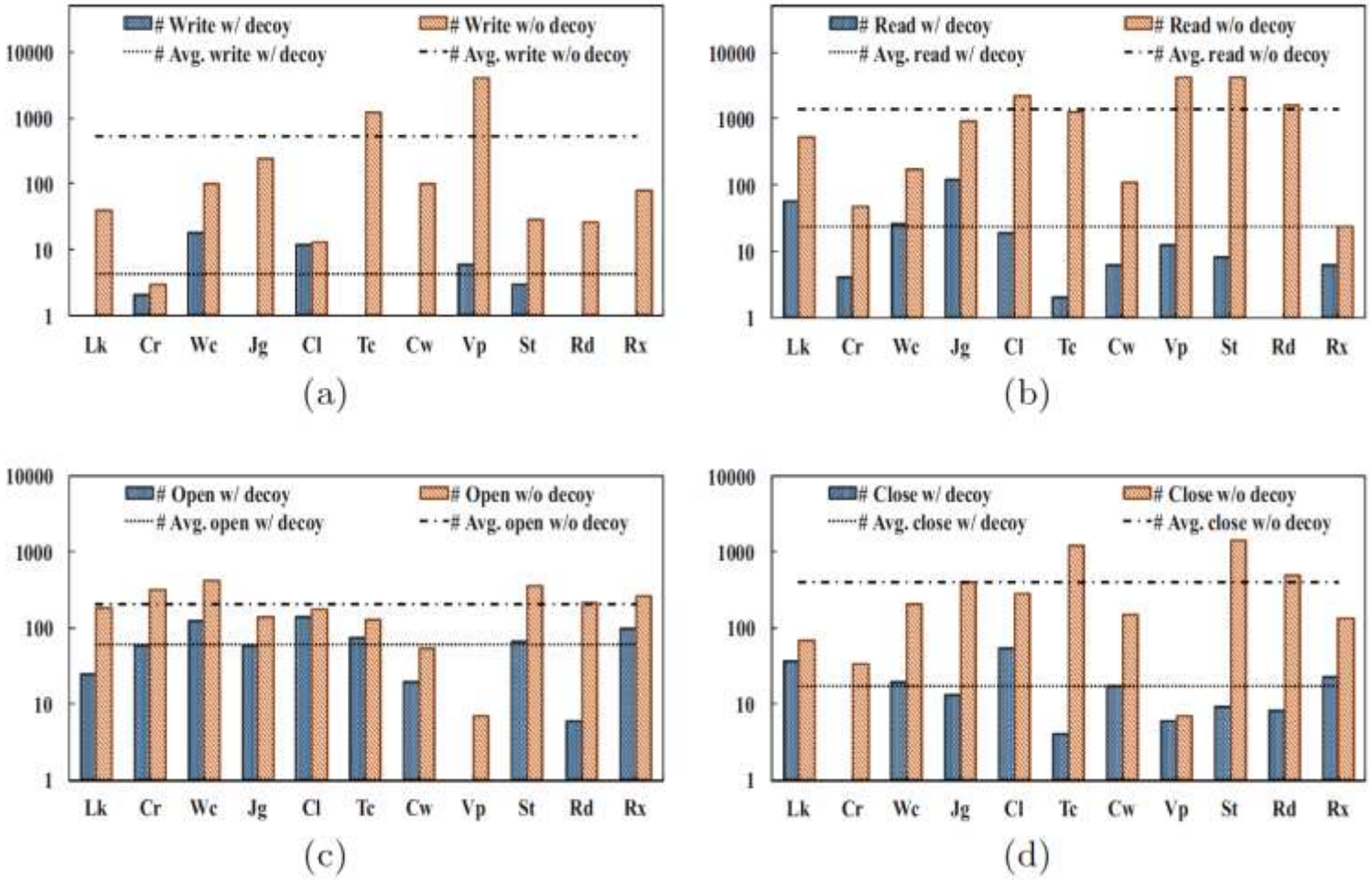
- RWGuard
  - different file change pattern of ransomware
  - solution: file change monitor based on *similarity*, *entropy*, and *file type*
  - limitation: users can encrypt files too
  - use all three solutions together - uses machine learning based models to detect based on the patterns

Crypto Ransomware

- RWGuard
  - evaluated RWGuard's performance using 14 most prevalent ransomware families
  - achieved real-time detection with 0 false negatives and 0.1/% false positive rate

Decoy monitor is the fastest detection mechanism

Number of Operations till detection

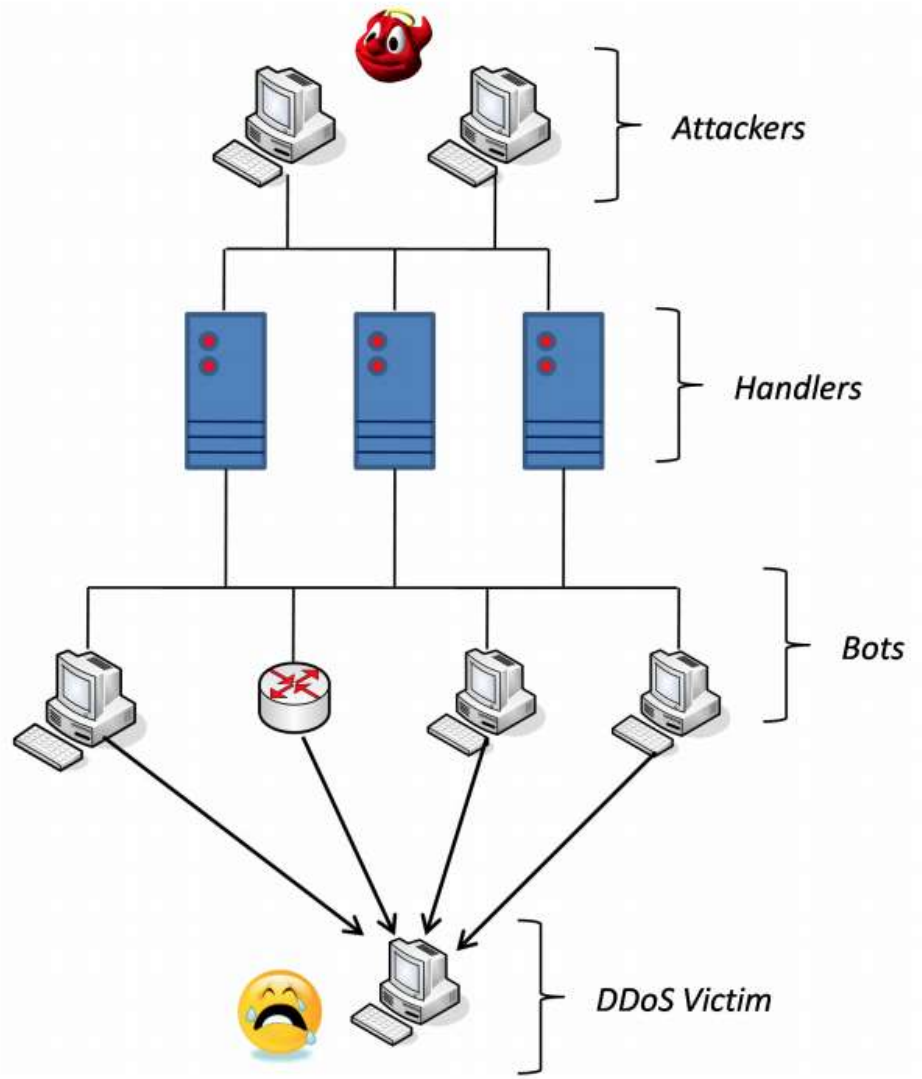


X-axis denotes different ransomware families

The Takeaway

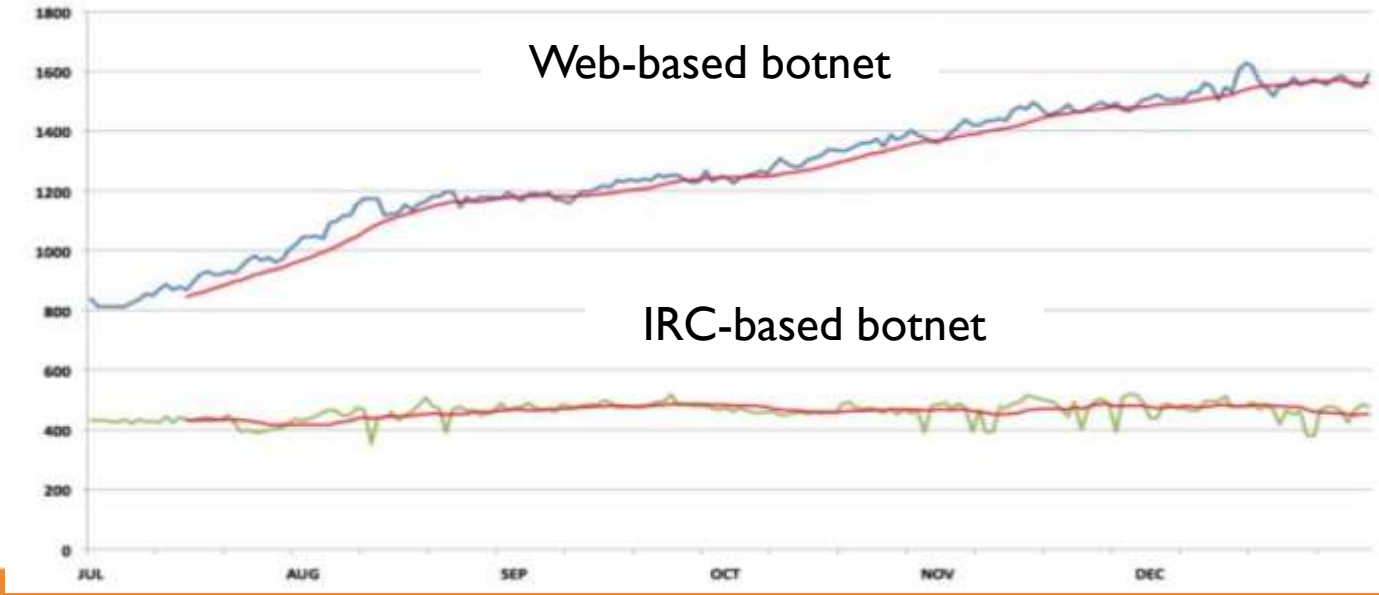
- Machine learning is a promising future direction for A/V

Botnet: How Does It Work?



Types of Botnets

- By handlers
  - IRC-based botnets: internet-relay chat (text-based protocol)
    - bots receive command from a single botmaster, single server easier to detect
  - Web-based botnets: uses HTTP/HTTPS protocols for communicating with bots
    - bots can communicate to multiple servers or hijacked legit websites - hard to take down

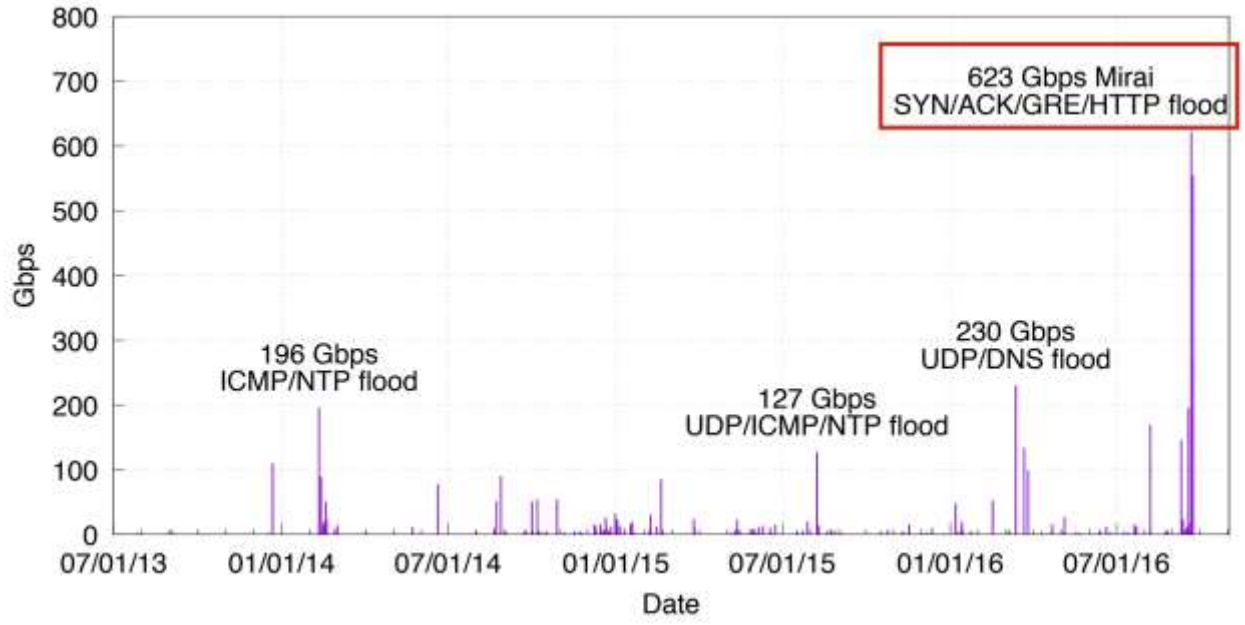


Mirai Botnet

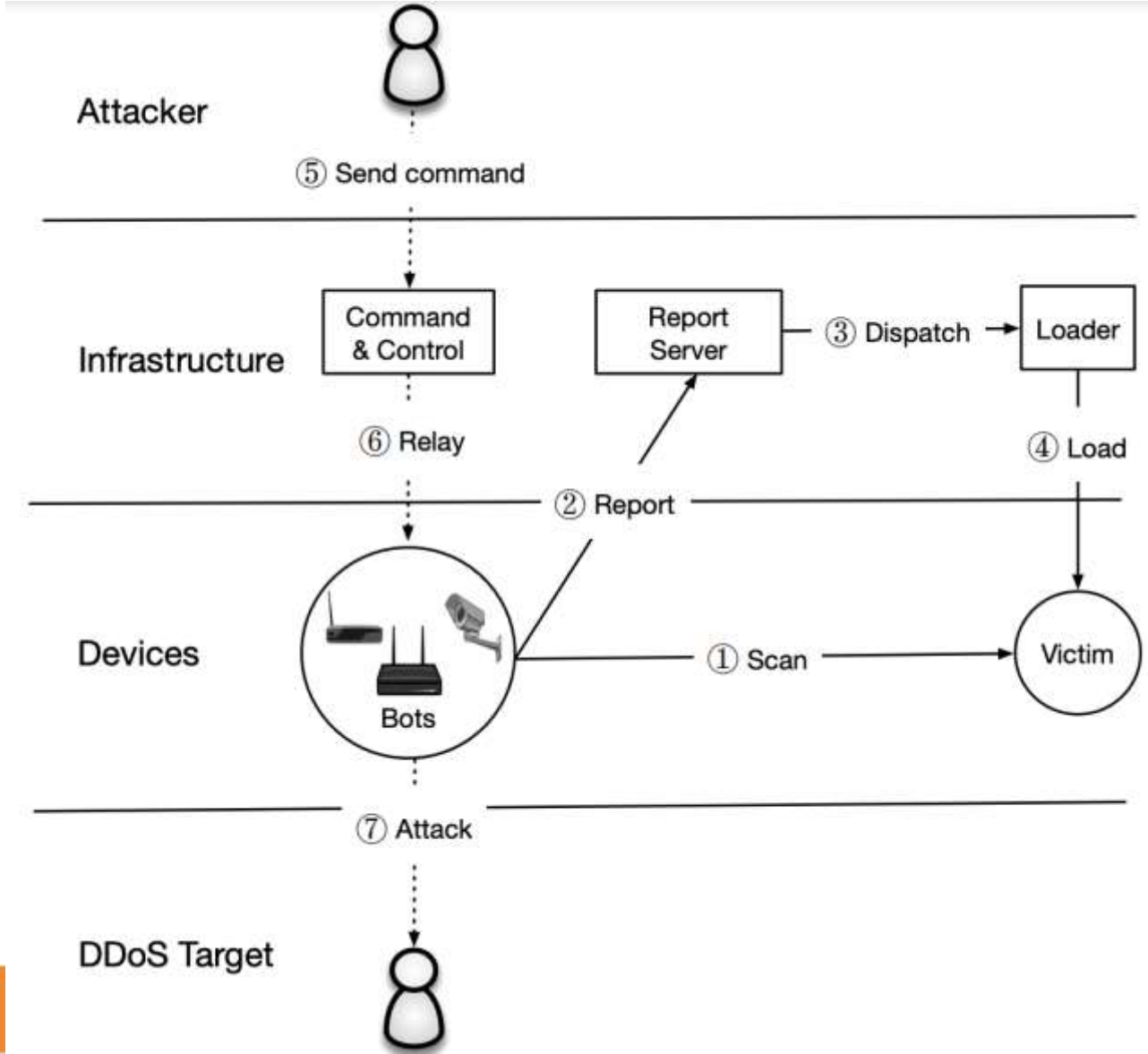
[Antonakakis et al., Understanding the Mirai Botnet, (USENIX'17)]

What is Mirai?

- A botnet consisting of 200K-300K globally distributed compromised IoT bots
- The enabler of the largest DDoS attacks ever recorded



Mirai Lifecycle



Mirai Timeline

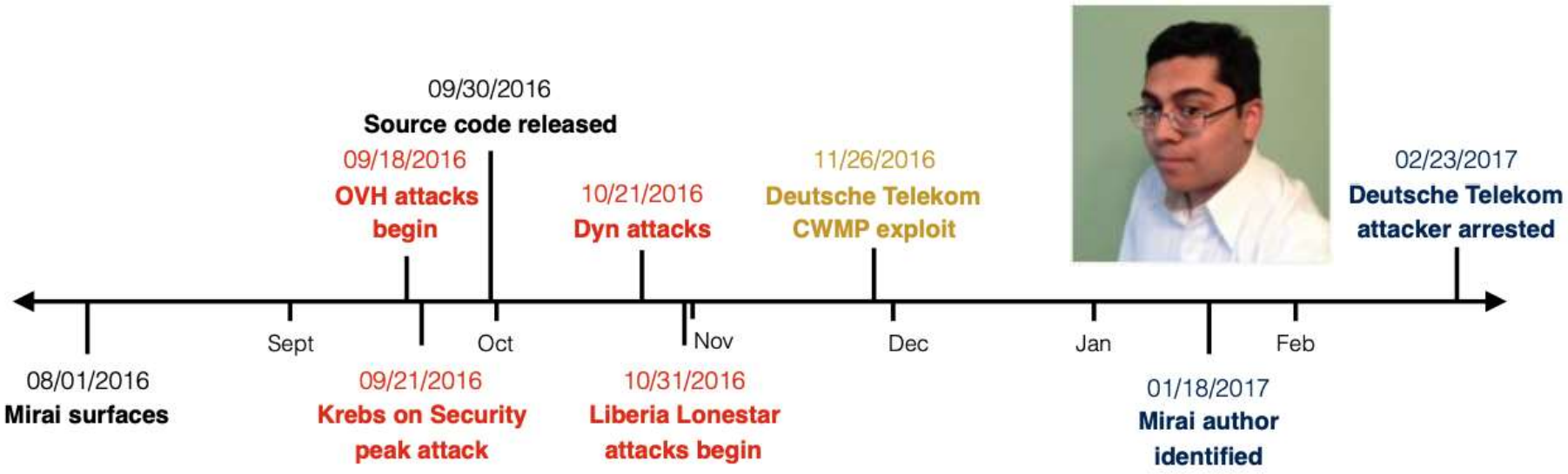


Figure 1: **Mirai Timeline**—Major attacks (red), exploits (yellow), and events (black) related to the Mirai botnet.

Major Targets

KrebsOnSecurity

Akamai

Project Shield

Major Targets

- Dyn DNS (domain name system) servers

Major Targets

- Games: Minecraft, Runescape, game commerce site
- Politics: Chinese political dissidents, regional Italian politician
- Anti-DDoS: DDoS protection service
- Matches victim heterogeneity of booter services
- Many clusters by a single operator; multiple operators behind attacks

Unconventional DDoS Behavior

- Current landscape of DDoS: 65% volumetric, 18% TCP state exhaustion, 18% application-layer attacks
- Mirai: 33% volumetric, 32% TCP state, 34% application layer (substantially differs from above)
- Limited amplification/reflection: 2.8% reflection, compared to 74% attacks are issued by booter services (attacks are already powerful)

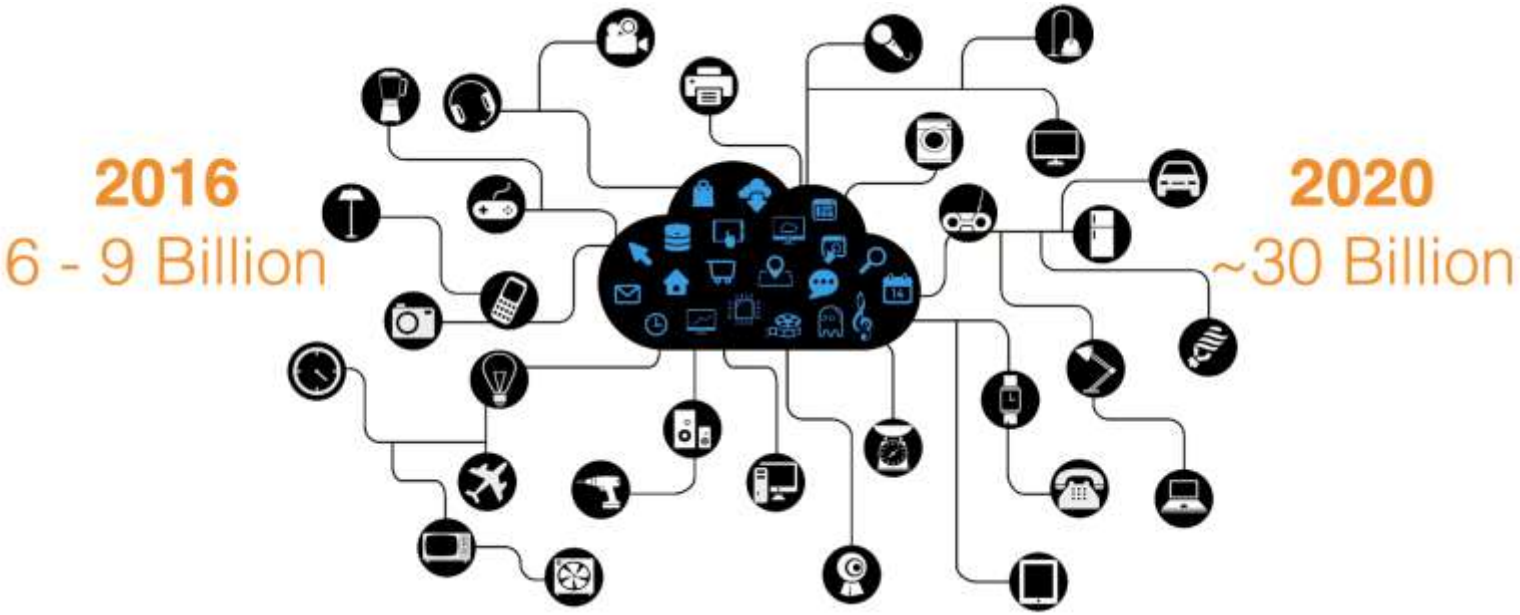
The Takeaway: Security Hardening

Password	Device Type	Password	Device Type	Password	Device Type
123456	ACTi IP Camera	klv1234	HiSilicon IP Camera	1111	Xerox Printer
anko	ANKO Products DVR	jvbzd	HiSilicon IP Camera	Zte521	ZTE Router
pass	Axis IP Camera	admin	IPX-DDK Network Camera	1234	Unknown
888888	Dahua DVR	system	IQinVision Cameras	12345	Unknown
666666	Dahua DVR	meinsm	Mobotix Network Camera	admin1234	Unknown
vizxv	Dahua IP Camera	54321	Packet8 VOIP Phone	default	Unknown
7ujMko0vizxv	Dahua IP Camera	00000000	Panasonic Printer	fucker	Unknown
7ujMko0admin	Dahua IP Camera	realtek	RealTek Routers	guest	Unknown
666666	Dahua IP Camera	1111111	Samsung IP Camera	password	Unknown
dreambox	Dreambox TV Receiver	xmhdipc	Shenzhen Anran Camera	root	Unknown
juantech	Guangzhou Juan Optical	smcadmin	SMC Routers	service	Unknown
xc3511	H.264 Chinese DVR	ikwb	Toshiba Network Camera	support	Unknown
OxhlwSG8	HiSilicon IP Camera	ubnt	Ubiquiti AirOS Router	tech	Unknown
cat1029	HiSilicon IP Camera	supervisor	VideoIQ	user	Unknown
hi3518	HiSilicon IP Camera	<none>	Vivotek IP Camera	zlxx.	Unknown
klv123	HiSilicon IP Camera				

Table 5: **Default Passwords**—The 09/30/2016 Mirai source release included 46 unique passwords, some of which were traceable to a device vendor and device type. Mirai primarily targeted IP cameras, DVRs, and consumer routers.

The Takeaway: Security Hardening

- ~35 billion IoT devices in 2021; ~75 billion by 2025



The Takeaway: Security Hardening

- Use best practices: random default password; default-closed ports at setup time (for network connection); ASLR; certification (to meet minimum security requirements)
- Automatic updates (need to consider resource constraints)
- Facilitating device identification (easy to locate infected devices)
- End of life (still remains a threat when long-term support is disabled)

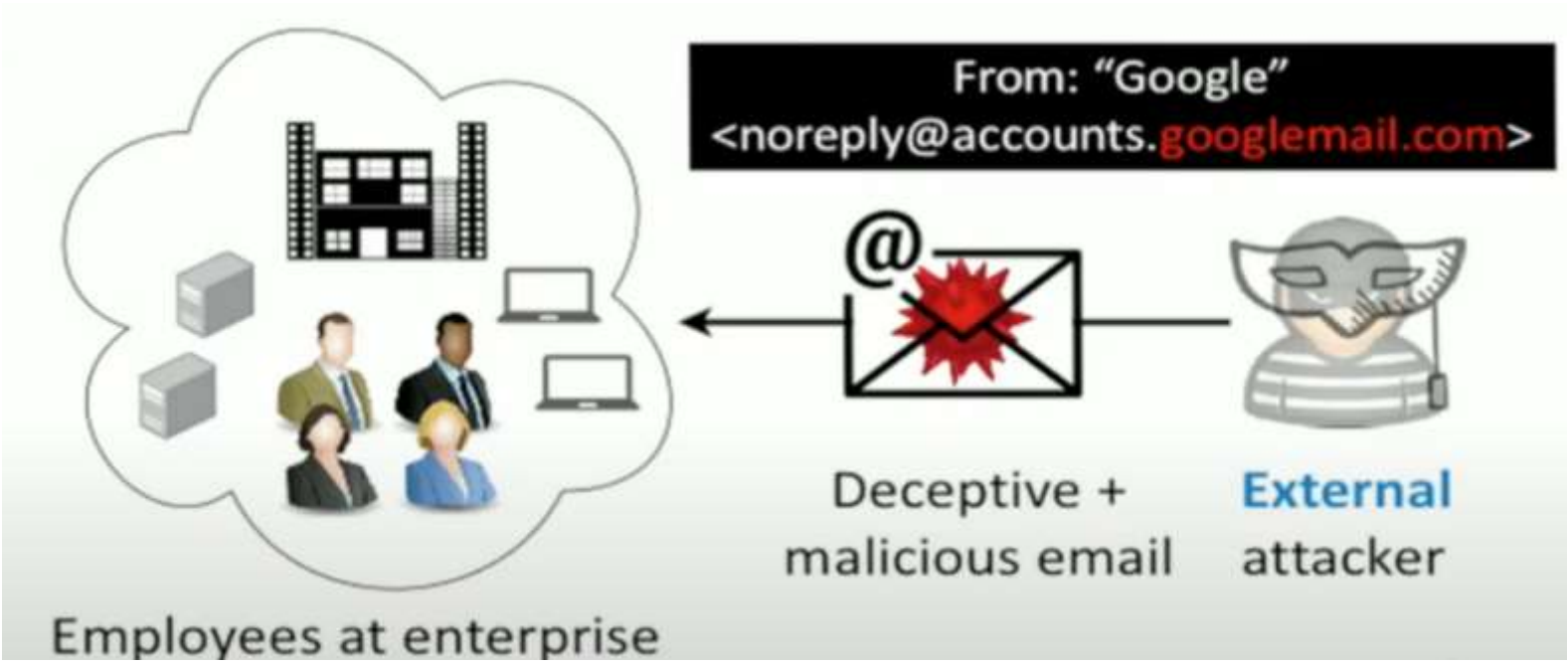
Phishing

[Ho et al., Detecting and Characterizing Lateral Phishing at Scale, (USENIX'19)]

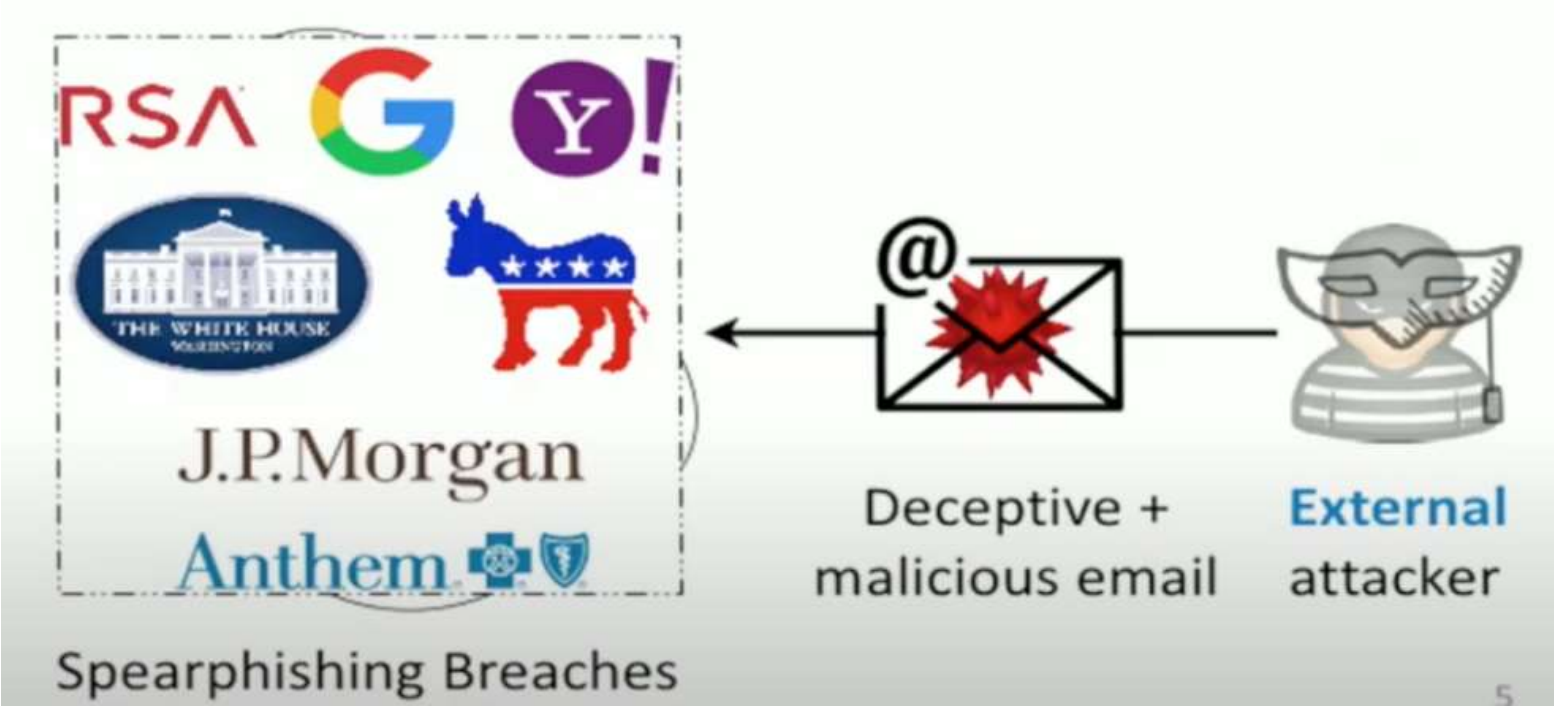
What Is Lateral Phishing?

- Attackers use a compromised enterprise account to send emails to other users
- Most stealthy phishing attack: exploits the implicit trust; uses information in hijacked account

Typical Mental Model

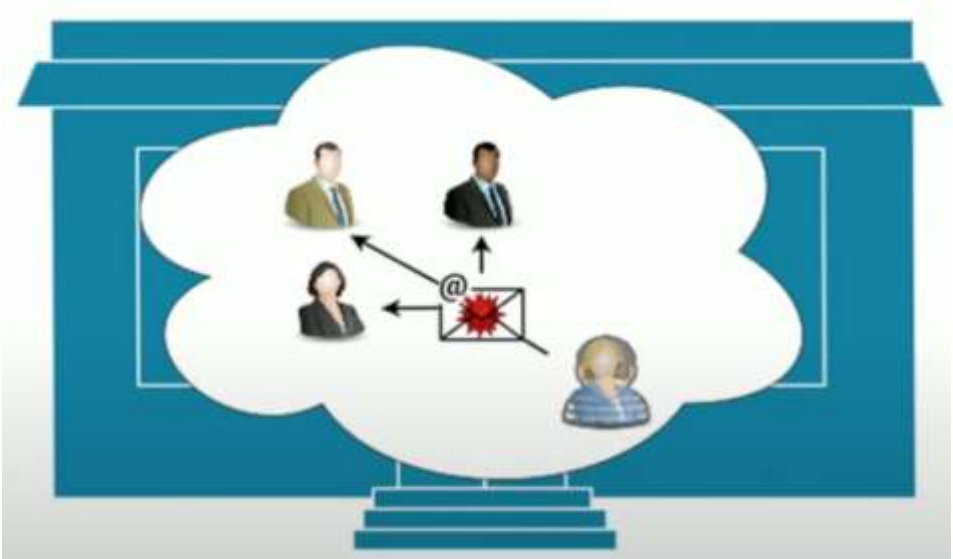


Typical Mental Model



Lateral Phishing: Attacks from Within

- Users and anti-phishing expects inbound attacks
  - Typically expects and prepares for attacks from externals
- No spoofing/forgery of sender metadata
- Compromised email+contacts for better targeting



Machine Learning-based Detector

- Extract features from and classify employee-*sent* emails
- Features: 3 categories
  - Lure: does the email contain commonly identified "phishy" words or phrases?
  - Exploit: does the email contain rare/unusual URLs (relative to global URL reputation system)?
  - Targeting: is the email sent to an unusual set of recipients (compared to past history)?

Detection Results

Attacks detected	**106 / 110 incidents (87%)** 49 incidents: no user reporting
False Positives	316 / 87.4 million emails: **Less than 4 / 1,000,000 employee-sent emails**

Widespread and Successful

- 1/7 randomly sampled organizations suffered from lateral phishing
- >10% of lateral phishers successfully compromised 1+ new employee account (underestimation)

Targeting: 2 Dominant Narratives

- Problem with the recipient's account or computer

> Dear user,
> We noticed an error on your account, kindly rectify below click here. Sorry for the inconvenience.

- Shared/new/updated document: >2/3 incidents

> Hello, please see attached invoice and packing list, confirm and advise. Thanks!

Targeting: Content Specificity

- Generic phishing message (63%)

"Please view the documents I sent you."

- Enterprise related (but generic) message (30%)

Hi team,

Please view the updated work schedule.
View document.

Thanks.

- Targeted message (7%)

Hi,

The attached file is the [Specific X] we use for [Project Y]. Please sign in securely to access the report.

Open [Hyperlinked Logo Image]

Attacker Sophistication

- Victims of lateral phishing responded to attack emails

"Did you mean to send this to me?"

"Can you tell me what this document is about?"

"I logged in to view it, but I don't understand why you sent this to me."

Attacker Sophistication

- 25% lateral phishers manually engaged with their recipients' replies

"Yes, have you checked it yet?"

"It is a document about [X]. It's safe to open. You can view it by logging in with your email address and password."

- 19% lateral phishers hid phishing activity from the account's real user, e.g., deleting sent emails

The Takeaway

- User awareness to mitigate social engineering attacks
- Machine learning is a promising future direction for A/V

How Can Malware Be Prevented

- Restricting what software users can install
- Better user education
- Eliminating software vulnerabilities
- Code signing (to prove authenticity)
- Industry-driven solutions: anti-virus, intrusion detection/prevention systems