Gavin Reid

But cyber!
Where are we with security in 2016?
DHS infosec chief: We should pull clearance of feds who fail phish test
Repeat offenders "should not be holding a TS SCI with the federal government."

by Sean Gallagher - Sep 21, 2015 12:00pm EDT

In the wake of the Office of Personnel Management hack this year, which reportedly took advantage of a phishing attack to steal credentials used to gain access to highly sensitive personnel records, US federal agencies have been increasing their security training and employee testing around phishing. In addition to the employee awareness campaign launched by the National Counterintelligence and Security Center, more agencies are using security auditing tools that simulate phishing attacks against employees to test whether the employees abide by their information security training. Those who fail for phishing tests are generally either required to take a security refresher class or at worst are publicly called out for their errors in agency e-mails.

But at least one federal chief information security officer thinks that these steps aren't enough and...
The state of the industry...
What we need to do differently...
What is threat?

What is intelligence?

intent, capability and opportunity
What can threat intelligence help you with?

Are we part of a new hack?

If the hackers reuse infra will notice and be able to take advantage of that?

IS this part of a larger campaign?

How did we get infected?

How do we know if we are completely clean of compromise?

Are we Targeted?

What has this IP done in the past?

Are we Targeted?
Indicators of Compromise...

“An IOC is an observable artifact of an intrusion on a host or network. Analysts can use it to trace the steps of an attack and identify what was affected, how long it was active or if there are any persisting elements of the intrusion.”

- Observables
- Measurable events
- Stateful properties
What is an indicator?

* Full list at [http://openioc.org/terms(Current.iocterms)](http://openioc.org/terms/current.iocterms)
IP with no (or invalid) context...

8.8.8.8
IP with context...better

Attachment MD5s:
b4fe7224da594703e78d62d9cb85c5f4c3a00c36
ea51040c3a10c557154bc7b15b9acbcd6555539
8a7e3fd0f0a389cf9582b75b4f8855dbe555bff08
0c57808abe699ba4855340adf5c9d7092e9df08b

Payload URLs:
hxxp://internetz1[.]com/03/39.exe
hxxp://gggrp[.]com/03/59.exe
hxxp://fefg[.]com/03/39.exe
hxxp://woofe[.]com/03/39.exe
hxxp://contestswin[.]net/03/39.exe

Payload MD5:
5e91af2e44c17de55134ff935c0f30f1

C2:
130.0.133[.]35

Malware: Dridex

Attachment File Name: RZZA3440.doc
Intelligence – best

Investigator finds new malware in word doc used in spearphish
– hashes file 7c47ff87c0frca93e135c9acffee48d3f
– Sandboxes and Finds c2

Query TI database (Intel 471) finds that same file/C2 has been used before by a specific hacker group X

Group X uses various hacker forums, IRC, samples, URLs and C2’s

Check nF for IRC connections to server. Runs the new IOCS into comparison engine and finds other infections – helping organization completely understand and fix the problem
Progression? of detection capabilities

- Exploit Sigs (IDS/HIDS)
- Getting hacked
- Anti Virus
- NBAD/nF
- DPI attack sigs (Yara)
- Logging
- SIEM
- PCAP
- Big Data/Analytics
- TTPs
- Nirvana
- IOCs
Feeds...
<table>
<thead>
<tr>
<th>Sources... (providers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry Orgs</td>
</tr>
<tr>
<td>Secret Groups</td>
</tr>
<tr>
<td>Vendor Threat Intel</td>
</tr>
<tr>
<td>First Party Data</td>
</tr>
<tr>
<td>Government Orgs</td>
</tr>
<tr>
<td>Peer Groups</td>
</tr>
<tr>
<td>Open Source</td>
</tr>
<tr>
<td>CIRTS</td>
</tr>
<tr>
<td>ISACS</td>
</tr>
</tbody>
</table>
What IS context?

- Start time?
- Impact?
- Who found it? (contact)
- Description?
- Data restriction?
- How was it found?
- Related activity?
- Confidence?
<table>
<thead>
<tr>
<th>Data Enrichment...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Whois</strong></td>
</tr>
<tr>
<td><strong>GeoLocation</strong></td>
</tr>
<tr>
<td><strong>Reputation</strong></td>
</tr>
<tr>
<td><strong>History</strong></td>
</tr>
<tr>
<td><strong>Hash</strong></td>
</tr>
<tr>
<td><strong>PDNS</strong></td>
</tr>
<tr>
<td><strong>VirusTotal</strong></td>
</tr>
<tr>
<td><strong>Sandboxing</strong></td>
</tr>
<tr>
<td><strong>Confidence</strong></td>
</tr>
</tbody>
</table>
Where does the data come from

- Customer data
- Scanning
- Web
- Malware processing
- Honeynets
- Human INT
How to eat them

Cybox

IOC

CSV

Raw
Operationalizing...Platforms

Providers
- Internet Identity
- Fox IT
- Intel 471
- iSight Partners
- ZuesTracker
- CriticalStack

Feed Manager
- Soltra
- ThreatGrid
- Crits

Integration
- Splice/Splunk
- SIM, Logger

Subscribed Controls

Internal Data
- IDS/IPS
- HIDS
- NetFlow

Decision
Is there a match?
How does Cisco do it

- Python/Django front end UI
  - Apache or Django runserver

- MongoDB backend
  - Fault Tolerant
  - High Performance
  - NO SQL
  - Mongo FS for files

- Document based
  - Files and metadata
What does CRiTs look like

### Top Backdoors

<table>
<thead>
<tr>
<th>Name</th>
<th>Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPD</td>
<td>1</td>
</tr>
<tr>
<td>PVY</td>
<td></td>
</tr>
</tbody>
</table>

### Top Campaigns

<table>
<thead>
<tr>
<th>Name</th>
<th>Emails</th>
<th>Indicators</th>
<th>Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 3</td>
<td>0</td>
<td>2067</td>
<td>1</td>
</tr>
<tr>
<td>Group 17</td>
<td>0</td>
<td>818</td>
<td>11</td>
</tr>
<tr>
<td>Group 16</td>
<td>0</td>
<td>68</td>
<td>0</td>
</tr>
<tr>
<td>Group 13</td>
<td>0</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>Group 10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Latest Indicators

<table>
<thead>
<tr>
<th>Value</th>
<th>Type</th>
<th>Date Added</th>
<th>Campaign</th>
<th>Source</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>mx.xmlflash.net</td>
<td>Domain</td>
<td>2013-11-14</td>
<td>Group 3</td>
<td>OTHER</td>
<td>New</td>
</tr>
<tr>
<td><a href="http://www.nbsd.k12.ms.us">www.nbsd.k12.ms.us</a></td>
<td>Domain</td>
<td>2013-11-14</td>
<td>Group 4</td>
<td>OTHER</td>
<td>New</td>
</tr>
<tr>
<td>/serv/pte.exe</td>
<td>Domain</td>
<td>2013-11-14</td>
<td>Group 4</td>
<td>OTHER</td>
<td>New</td>
</tr>
<tr>
<td>2014 individual income tax credit policy</td>
<td>String</td>
<td>2013-11-14</td>
<td>Group 4</td>
<td>OTHER</td>
<td>New</td>
</tr>
</tbody>
</table>

### Recently Added/Modified Samples

<table>
<thead>
<tr>
<th>Filename</th>
<th>Size</th>
<th>Filetype</th>
<th>Receive</th>
<th>Backdoor(v)[C]</th>
<th>CVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>jack246.exe</td>
<td></td>
<td></td>
<td>08/12/2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sample</td>
<td></td>
<td></td>
<td>08/12/2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c5eb1c6f314e4d682b1315dfab44e7dd</td>
<td></td>
<td></td>
<td>08/12/2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sample</td>
<td></td>
<td></td>
<td>08/12/2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>68bee94684ba33d1e5d97d7d27d0fe13.exe_carver</td>
<td></td>
<td></td>
<td>08/12/2013</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What about techniques

wmic /node:"@server-targets.txt" service get name

wmic /node:"machine-FQDN" service get name
So what could you do

C:\>wmic qfe get HotfixID,ServicePackInEffect,InstallDate,InstalledBy,InstalledOn /format:csv

Node,HotFixID,InstallDate,InstalledBy,InstalledOn,ServicePackInEffect
GAVREID-178C,KB2849697,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2849695,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2844134,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2670838,,NT AUTHORITY\SYSTEM,2/5/2015,
GAVREID-178C,KB2838477,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2592687,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB971033,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2819745,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2479943,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2491683,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2506014,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2586212,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2506928,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2509553,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2511455,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2515325,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2533552,,NT AUTHORITY\SYSTEM,2/5/2015,
GAVREID-178C,KB2533523,,NT AUTHORITY\SYSTEM,2/5/2015,
GAVREID-178C,KB2534111,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB2534270,,GAVREID-178C\Administrator,2/5/2015,
GAVREID-178C,KB25356270,,GAVREID-178C\Administrator,2/5/2015,
## Powers(hell)

<table>
<thead>
<tr>
<th>Set-ExecutionPolicy</th>
<th>Mimikatz</th>
<th>EncodedCommand</th>
<th>Find-AVSignature</th>
</tr>
</thead>
<tbody>
<tr>
<td>DllInjection</td>
<td>Invoke-Shellcode</td>
<td>Get-Keystrokes</td>
<td>Get-TimedScreenshot</td>
</tr>
<tr>
<td>Invoke-CredentialInjection</td>
<td>Invoke-PSInject</td>
<td>Invoke-ServiceStart</td>
<td>Get-RegAutoLogon</td>
</tr>
<tr>
<td>Add-ScrnSaveBackdoor</td>
<td>Invoke-ServiceUserAdd</td>
<td>Write-ServiceEXE</td>
<td>Invoke-TokenManipulation</td>
</tr>
</tbody>
</table>
Empire is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework.
PowerShellEmpire Agent

Tracking Evolution of the PowerShell Empire Agent and discussion in Chinese Forums

Translated from Chinese: "If the listener does not specify an executable file, the program may enable the default cmd.exe instead:"

@secure_sean PowerShell Empire - a pure #PowerShell post-exploitation agent.
Making it intelligent

What do you do with this data to help your organization

• Detecting this technique means logging WMIC & Powershell
• Pull logs from at least your server environment
• Whitelist know good and alerting on all else
• Empire commands get investigated immediately
Maturity...

Low: most indicator-based; IP-based blocking; only able to consume tactical products.

Medium: indicators are grouped and have context; Indicator to internal data comparisons automated. Mix of 3rd party with some first party

High: production of unique and relevant products for different internal customers; Used for prioritization of security arch. Automatic subscription of high fidelity data to security controls. HI-FIDELITY FIRST-PARTY
Can you protect what you can’t see?
Thanks!