Innovations in Cybersecurity

TAG 2018 Conference
Purpose and Expected Outcomes

We Discuss
• Security Approaches
• Recommended Practices

You Take Away
• Security Framework
• Implementation Ideas
You Need a Plan
Walk Before You Innovate

Require Strong Passwords (Psst: MFA)

Keep Your Systems Patched

Train Your Users on Phishing
Jim Rutt

CIO, Dana Foundation
CISSP, CISM, CISA, CGEIT, CRISC, C|CISO
Dana State: 2010

- Key Security Controls:
  - VPN (JUNOS)
  - Basic Antivirus (McAfee)
  - MS Exchange Protection (Trend Micro, McAfee Continuity Solutions)
  - Segmentation between VMWare virtual machines (manually applied via rule)
  - Active Directory (integrated with Exchange)
Dana State: 2018

- CASB (Netskope)
- O365 Native Continuity
- Advanced Antimalware (Minerva)
- Advanced Data tracking (Cyberhaven)
- Critical File Encryption (Vera)
- New System of Record for Identity (Okta)
- UBEA (User Behavioral Analytics)-Preempt
Dana State: Beyond 2018

- Zero-Trust Networks/CARTA (as defined by Gartner)
- SOAR (Security Operations, Analytics, and Reporting)
- Network As A Service (NaaS)
Zero Trust Networking

• Prevents lateral movement within networks
• One key driver is micro-segmentation (samples: vArmour, Illumio)
• Breaks away from traditional perimeter defense posture
• Assumes threat actors are already in proximity.
CARTA (Continuous Adaptive Risk and Trust Assessment)

Figure 1. Seven CARTA Imperatives

1. Replace one-time security gates with context-aware, adaptive and programmable security platforms.
2. Continuously discover, monitor, assess and prioritize risk — proactively and reactively.
4. Instrument infrastructure for comprehensive, full-stack risk visibility, including sensitive data handling.
5. Use analytics, AI, automation, and orchestration to speed the time to detect and respond and to scale.
6. Architect security as an integrated, adaptive programmable system, not silos.
7. Put continuous data-driven risk decision making and risk ownership into BUs and product owners.

Source: Gartner (April 2018)

Sample providers: Wootcloud, Armis, Centrify
SOAR (Security Operations, Analytics, and Reporting)

- Use and expansion of use of SIEM (Security Incident and Event Management) to collect, correlate and analyze incidents
- Creation of incident workflows for reporting
- Reduction of reliance on SOC analysts, who are hard to recruit and even harder to train
- Sample providers: Phantom, Demisto, Siempify
Network As A Service (NaaS)

- Enhances and enables zero-trust methodologies on the network side
- Software
- Focused on intelligent analysis of demarcation points at the application level, not just IP level
- Examples: Meta, Luminate, Zscaler
Charles Richardson
CTO, The Heinz Endowments and Heinz Family Office
Private Cloud Infrastructure
A Co-Managed/Monitored Model
Data-Driven Computer Security Defense

• Intelligence-Based Defense
• Have an Offensive Posture
• AntiVirus is Not Enough
• Implement the Latest Password Guidelines
• Teach Users About Threats
• Have an Incident Response Plan
• Assume You Have Been Breached
• Focus on Root Causes
• Be Willing to Discard What Does Not Work

Source: (Grimes, 2018)
Windows zero-day flaw allows arbitrary file deletion

Oct 26, 2018

On October 23, 2018, Secureworks(R) Counter Threat Unit(TM) (CTU) researchers became aware of a Twitter post describing an unpatched flaw in Microsoft Windows. The vulnerability resides within the Data Sharing Service (DaSvc) component present in Windows 10, Windows Server 2016, and later versions. Using version 3 of the Common Vulnerability Scoring System (CVSSv3), an open standard for rating vulnerabilities, CTU(TM) analysts assigned the vulnerability a base CVSS score of 9.8 and a temporal score of 6.4.

The DaSvc component implements several remote procedure call (RPC) functions within dasvc.dll, including the vulnerable RpcDSSMoveToSharedFile function. This service, which runs with LOCAL SYSTEM privileges, can be accessed using advanced local procedure call (ALPC) messages from unprivileged processes. The vulnerable function allows the deletion of arbitrary files from the system.

A functioning publicly available proof-of-concept (POC) exploit deletes the pctl.sys driver from the Windows directory, rendering the system unbootable. The code can be trivially modified to delete other files on the system.

Threat actors could leverage the vulnerability to perform the following tasks:

- Make the system unstable by deleting critical operating system or program files.
- Lower the security posture of the system by deleting components of endpoint detection and response (EDR) or antivirus (AV) products.
- Delete a program library and replace it with a malicious library, exploiting DLL search-order hijacking and causing a signed or privileged executable to execute the malicious library.
- Delete configuration or other data stored in the system's temporary directory and owned by sensitive processes. An unprivileged user could then reconstrue these deleted files with malicious data to manipulate the behavior of the targeted application or service.

Detecting exploitation of this vulnerability is difficult in most situations. The Event Tracing for Windows (ETW) facility within Windows can be used to observe ALPC messages, including messages between the exploit code and the Service Host (svchost.exe) process hosting the DaSvc service (see Figure 1).
An Offensive Posture
AntiVirus Is Not Enough
Teach Users About Threats

![Training Campaigns](image)

<table>
<thead>
<tr>
<th>Campaign Name</th>
<th>Groups</th>
<th>Content</th>
<th>Complete %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed KAK</td>
<td>Newbies</td>
<td>2016 KnowBe4 Security Awareness Training 30min</td>
<td>100% Completed</td>
</tr>
<tr>
<td>07/05/2018 - 08/05/2018</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Completed KA</td>
<td>Newbies</td>
<td>2016 KnowBe4 Security Awareness Training 30min</td>
<td>100% Completed</td>
</tr>
<tr>
<td>12/11/2017 - 01/11/2018</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Completed NewHires</td>
<td>Newbies</td>
<td>2016 KnowBe4 Security Awareness Training 30min</td>
<td>100% Completed</td>
</tr>
<tr>
<td>10/02/2017 - 11/02/2017</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Assume You Have Been Breached

- Top Priority Breaches: 1,459
- Active Net Breaches: 218
- Easily Exploitable: 1,799
- Predicted Exploitable: 0
- Malware Exploitable: 38
- Popular Targets: 2,395
- Zero-Day Vulns: 0

Assets: 844
Vulnerabilities: 10,566
Fixes: 396

- 1,000: s-ex17w02ht5f9q
  - Score: 1,000
  - Locator: Windows XP
  - OS: Windows XP

- 1,000: genetecdc.heinz.local
  - Score: 1,000
  - Locator: Windows 2008 R2/7
  - OS: Windows 2008 R2/7

- 1,000: sv16-paris.heinz.local
  - Score: 1,000
  - Locator: Windows 2008 R2/7
  - OS: Windows 2008 R2/7

Linda from Kenna
Important Download Changes Coming!!!!! Over the course of the next 3-4 weeks, exports from...

Linda from Kenna
New Features Live! Total Fix Count Fix count tells you the number of missing patches, but...
Be Willing to Discard What Does Not Work

PRODUCT

CyGlass is a Software as a Service (SaaS) application that identifies, detects and responds to network-based cyber-attacks in real-time by leveraging our advanced layered AI approach. Using an ensemble of algorithms, CyGlass learns the customer’s network and can detect threats of unknown origin without requiring the set-up of rules or policies.
Question
Time
Thank You!

Complete Your Evaluation!