NATIONAL CYBER SUMMIT

June 4-6, 2019 | Huntsville, AL

Faster than the Speed of Threat:
Edge-to-Edge Cybersecurity

True Cyber Crime Story:

Blocking A Nation-State Attack

Byron DeLoach,
Director of Adaptive Solutions, Cybriant

Byron DeLoach

Byron has over 26 years of experience in the design and implementation of technical infrastructure and the management of technical service teams.

As Director of Adaptive Solutions for Cybriant, he is responsible for the operation and delivery of all managed services including 24/7 Managed SIEM with Live Security Monitoring, 24/7 Managed Endpoint Detection and Response, and Managed Patch and Vulnerability Management.

Blocking a Nation-State Actor

The FBI called (***again)*** to inform our customer's CTO that their organization was leaking data to a party in China. Here's a timeline of what happened before they called Cybriant:

Recipe for Disaster

Recipe for Disaster

Customer purchased and installed Carbon Black.

The product was hastily installed.

The customer stopped monitoring the product because they didn’t understand the events or how they effected their environment.

As a result the adversary stopped Carbon Black’s services, flow of data continued.

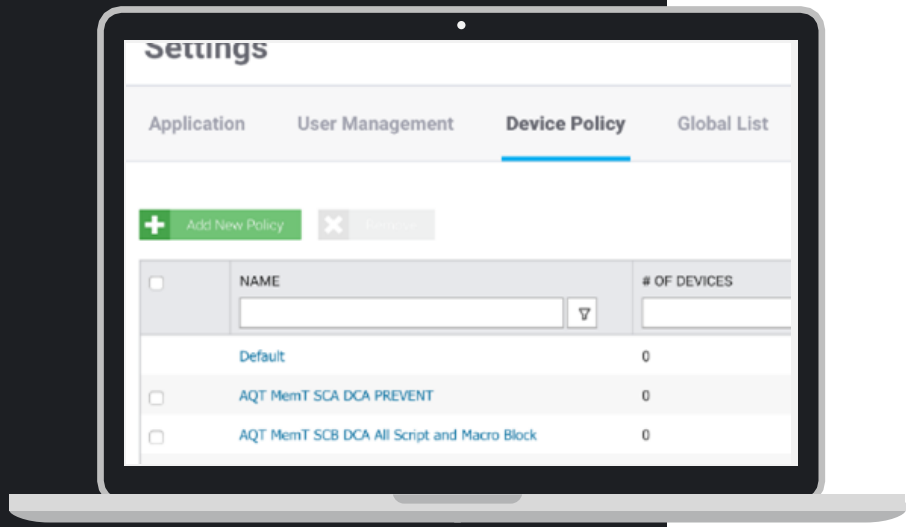
The calls from the FBI continued.

Choosing Cylance®

The customer was wary of “Next Generation Antivirus” solutions after their expensive Carbon Black failure.

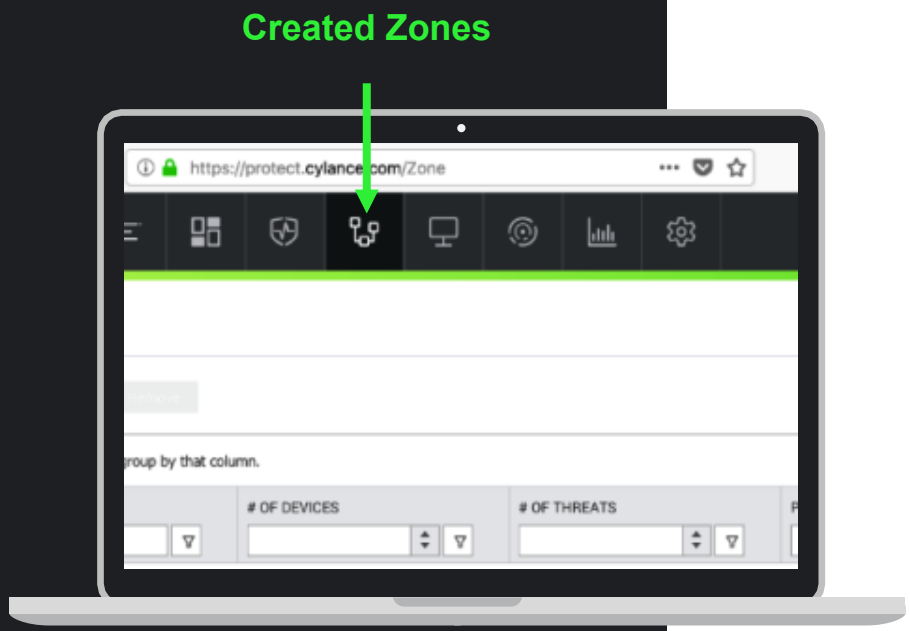
The customer demanded something that would be effective and would not stop business functions.

Easy choice…



Cylance Environment Prep

- Scorched earth approach.
- Stop everything and ask questions later.

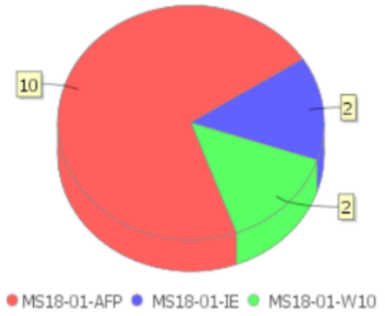


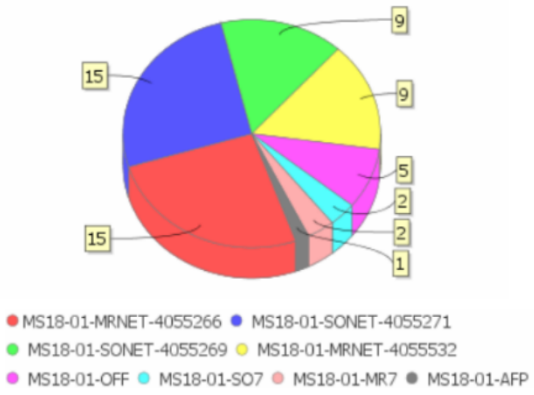
Cylance Environment Prep

- This is a convenient method to ensure that every system has a policy that does what is needed.
- Used Client's Active Directory naming convention

Nightmare Discovery

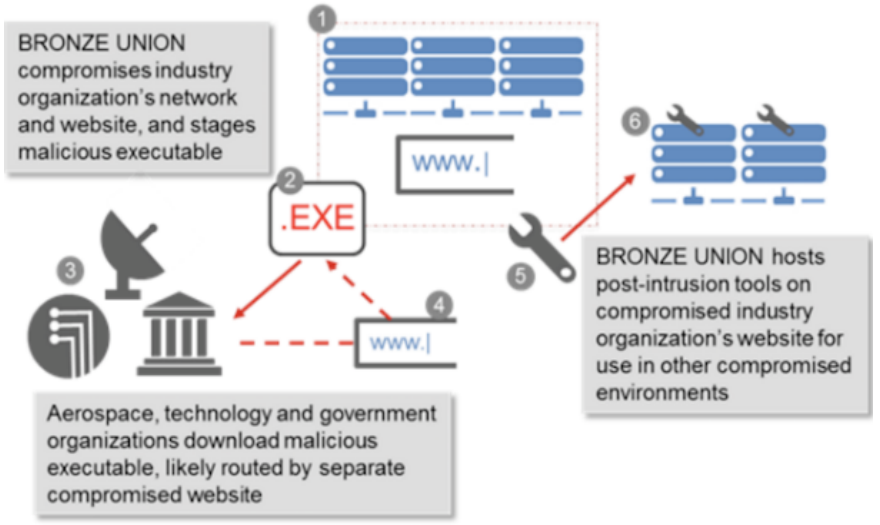
1. Began installing CylancePROTECT® on **unpatched** Exchange 2010 server.
2. CylancePROTECT **immediately** identified and quarantined a compromised version of owaauth.dll.
3. The Exchange server **stopped authenticating** users.
4. We were forced to continue to use the module until a replacement could be found.





Bad Guys Identified

The SHA 256 hash of the bogus owaauth.dll is associated with the group Bronze Union, (formerly labeled TG-3390) believed to be based in the People's Republic of China.



Nation-State Hackers Are Real!

- In 2014, the U.S. Government issued an indictment for five Chinese military hackers for cyber espionage.
- The Chinese military hackers stole intellectual property.
- Chinese solar panel makers were able to leapfrog technologies without the inconvenience and expense of research.
- Anticipate American regulators response in international trade disputes.

China Chopper

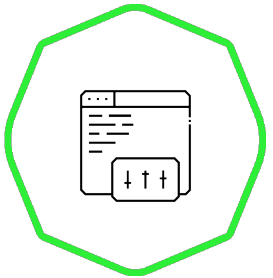
With stolen credentials using a combination of China Chopper (asp version) with the owaauth.dll on the exchange server, the adversary was able to:

Enable NTLM previous password support.

Enable and disable file shares as needed.

Use PowerShell console and scripts.

Use PSExec to distribute software.

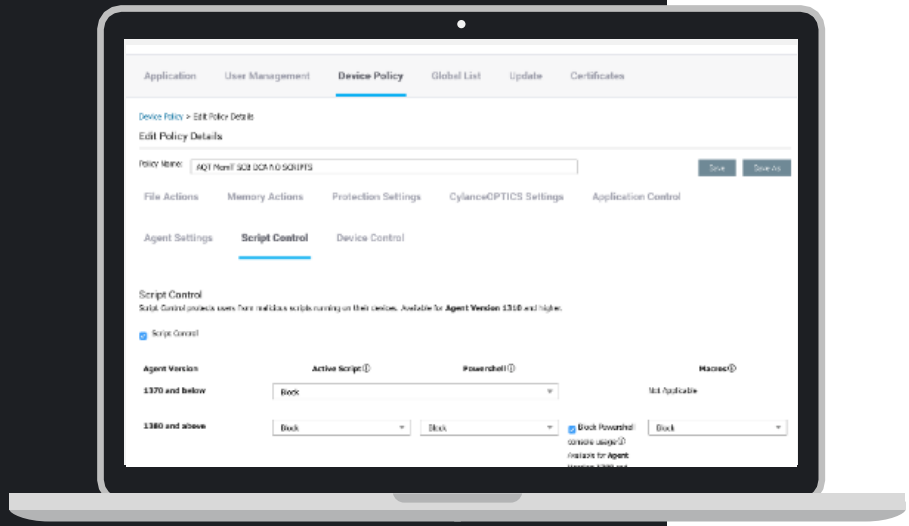


Add tasks to Task Scheduler.

With privileged credentials, the adversary started distributing batch files, PowerShell scripts, and software.

China Chopper

- The adversary has access to the goods. Now, they need to send them home.
- To do this, they distributed files to key systems.
- They used a combination of native windows functions, trusted applications, and configuration changes to accomplish their goal.

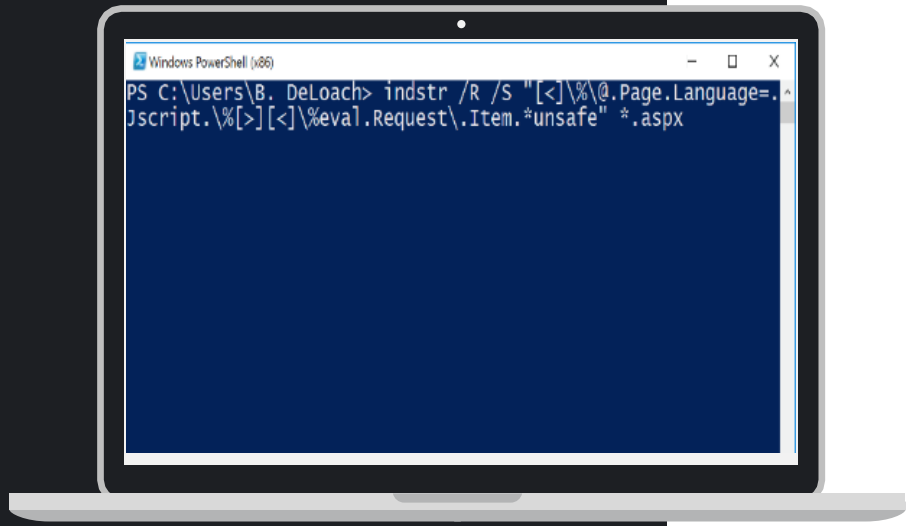


Our Mission

Our Mission: Stop bad guys from using PowerShell Console.

How We Achieved Our Mission:

- CylancePROTECT policies with Script Control.
- CylanceOPTICS™ rules to terminate Powershell downloads, hidden Powershell execution, and Powershell encoded commands.



Searching for China Chopper

Next, we searched every directory on the Exchange 2010 server for webshells, specifically China Chopper, using the findstr command and eliminated it from the system.

What Was Discovered

The adversary had been staging data using rar.exe, which they artfully re-named svchost.exe. However, they stored this file in the Recycle Bin.

Blocking This Activity

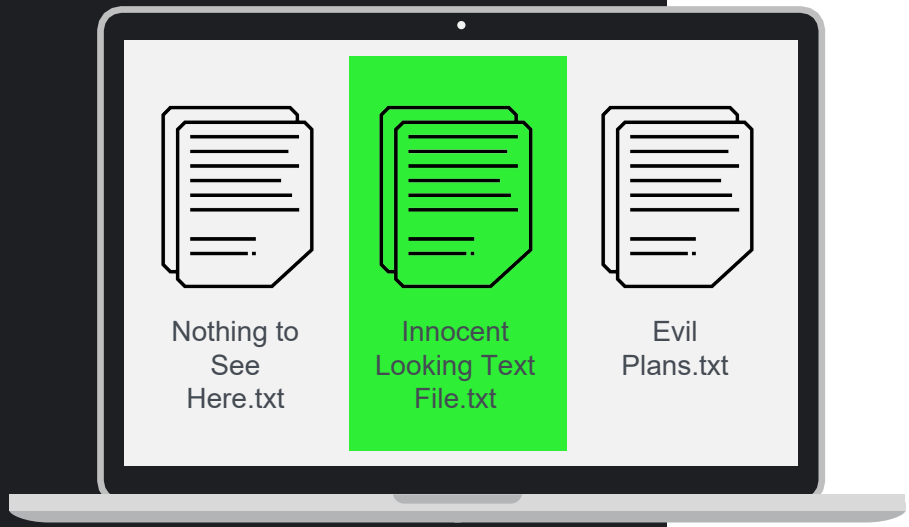
CylanceOPTICS rules can be used to block this type of activity	
Executable launched from Recycling Bin rule should be enabled with the following responses:	▪ Terminate Process ▪ Dump Detection To Disk
Optional:	▪ Log Off Remote Users ▪ Notification Window To Alert Local User of the Issue

Global Quarantine

CylanceOPTICS stopped executables from running in the Recycle Bin. This addressed our initial rar.exe problem, but they could still run it from other locations. To keep this powerful tool out of their hands, we needed to go one step further.

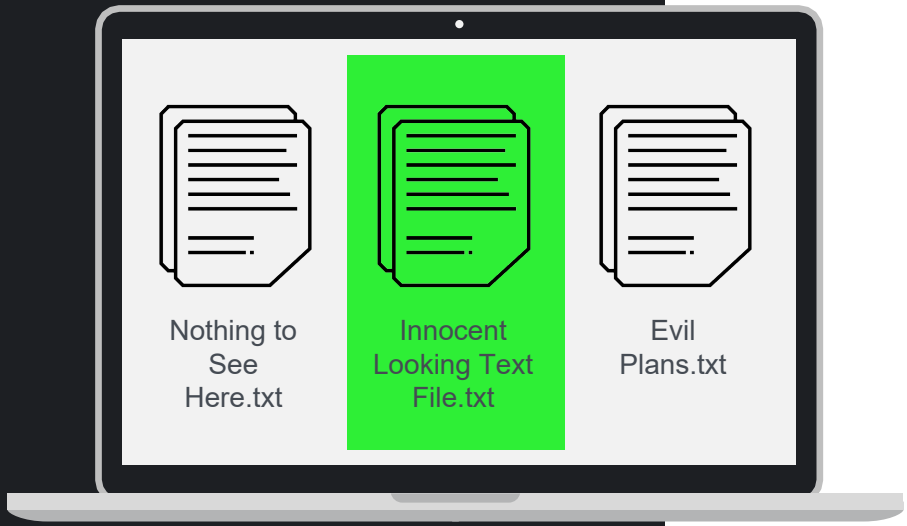
We used a combo of CylanceOptics and Protect to create a Global Quarantine of the file:

- Start an InstaQuery in CylanceOPTICS using the file name as the Search Term.
- Set the Artifact as File.
- Use the default Facet.
- Add the proper zones and submit the query.
- Use the results to globally quarantine your target file - no matter what they name the file, it will be quarantined.



Attack Phase 2

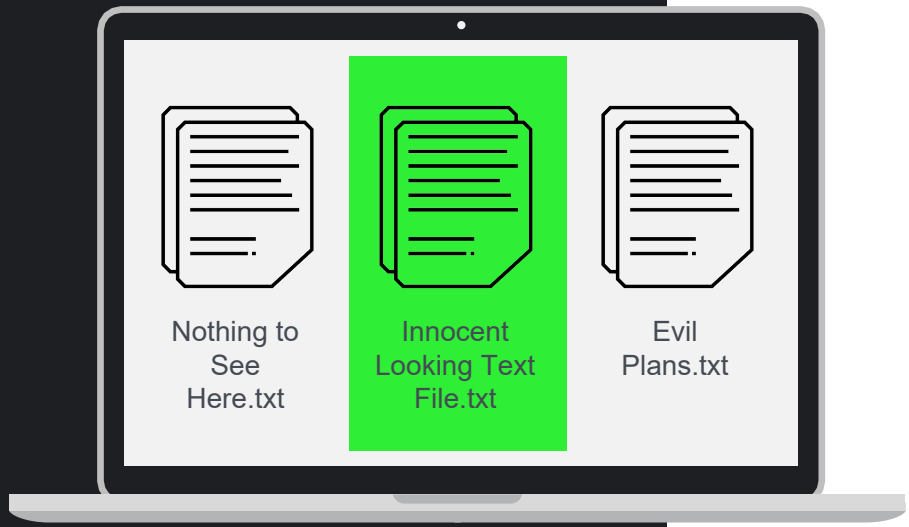
- With Powershell blocked, the adversary had to use other native Windows tools to hide and move data.
- They were very resourceful and our efforts only slowed them for a short time.



Compartments are not easily discovered unless the analyst knows to look for them. A very simple but effective way to hide data.

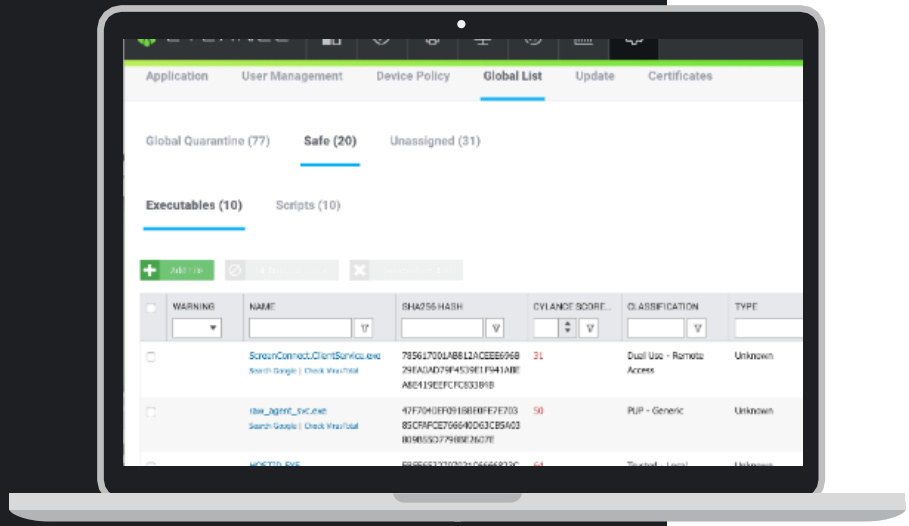
Attack Phase 2

- Notepad and batch files became the tools of choice. Notepad was used to stream data to secret text file compartments.
- They would then use .bat files to transfer their ill- gotten gains from system to system until they reached the P0wned Exchange server.



Attack Phase 2

- Luckily, the bad guys were only using Notepad on Windows 2008R2 servers. We were able to pre-form a CylanceOPTICS InstaQuery to locate and quarantine notepad.exe.
- As notepad.exe on the servers is a different version from Windows 10 workstations, our actions didn't take any useful tools away from the end-users.

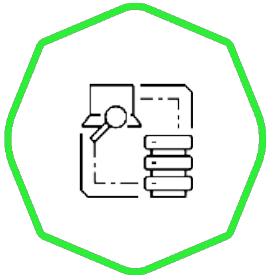


Each program was vetted and either approved or denied.

Attack Phase 2

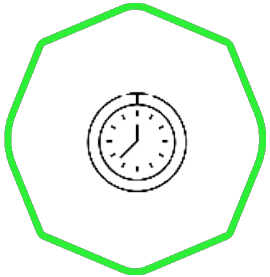
- After the excitement was over, we started the process of waiving or marking files safe that the business needed.
- We went through the process of sandboxing several of the programs and giving the customer reports so that they could make a decision with a balance of security and business needs.

The Not So Sexy Part…



Firewall Rules

We worked with the customer on setting up firewall rules to disallow SMB traffic to the Exchange server located in the AWS GovCloud.



Time-Consuming Tasks

Patching, changing firewall rules, testing and changing passwords is a time-consuming task that no one appreciates.

Question and Answer