



Reversing the Kill Chain

An Actionable Framework for defending against common threats

Amanda Berlin

NetWorks
GROUP

By a show of hands how many of you here have heard of the cyber kill chain, aka the Intrusion kill chain by lockheed martin?

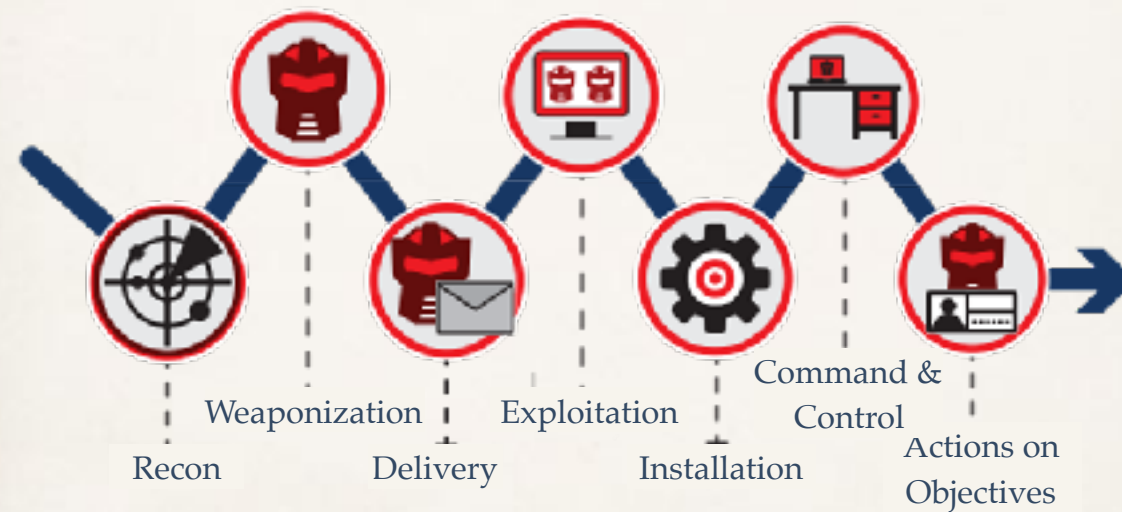
Ok, now how many of you can list the 7 different steps in the kill chain?

Awesome, so now, how many of you could give me a specific threat and what technically happens during each of those steps?

Well at one point I couldn't, and honestly still can't for some threats. I had struggled to show how the kill chain could be effectively used and applied in a real world example of the threats we face day to day.

I work in an mssp and have customers that craft their defenses around use cases, and have an idea of "yea sure I want to stop ransomware" but no fully articulated plan on what exactly that looks like. So today I want to give a little overview of the Intrusion Kill Chain, and then move on to an example of these use cases. Sometimes threats and attack methodologies don't fit into the kill chain and we'll go over that as well. We'll go over the specific pieces and parts of the attack at each step, what defensive mitigations you can implement to protect against them, and monitoring and alerting to go along with them as well.

Intrusion Kill Chain



The Intrusion Kill Chain, sometimes called the Cyber Kill Chain, is “a model for actionable intelligence when defenders align enterprise defensive capabilities to the specific processes an adversary undertakes to target that enterprise.”

So targeted attacks, APTs or whatever you want to call them.

It is composed of seven steps as described in the Lockheed Martin whitepaper:

1. Reconnaissance: Is when the attacker Researches, identifies and selects targets. They crawl Internet websites and look for mailing lists, email addresses, social relationships, or information on specific technologies. A big resource for this is LinkedIn and previous breaches.
2. Weaponization: The automation of some type of remote access tool or trojan, coupled with a malicious payload. Coupling a remote access trojan with an exploit into a deliverable payload. Files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.
3. Delivery: Transmission of the weapon to the targeted environment. The three most common delivery vectors are email attachments, websites, and USB drives.
4. Exploitation: After the payload is delivered, exploitation triggers the code. Most often, the exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or even a feature that auto-executes code.
5. Installation: Allows the adversary to maintain persistence inside the environment.

Common Threats

So what are some common threats that you can think of that are at the top of most people's minds when creating a plan for defense?

Things like ransomware, DDoS, data exfiltration, etc

According to this year's Version DBIR 88% of breaches fall into 9 categories. These 9 categories were listed back in 2014 and they are still what most of us worry about today.

1. Cyber-Espionage - Attacks linked to state sponsored actors and usually what people like to use as an excuse for most attribution.
2. Denial of Service - 98% are targeted towards large enterprises
3. Crimeware - Ransomware has climbed from the 22nd most common form of malware, up to the 5th in less than 3 years.
4. Insider privilege and misuse
5. physical theft and loss
6. web app attacks
7. misc errors (kind of like the typo that brought down amazon?)
8. payment card skimmers, PoS intrusion
9. everything else

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Specific Alerting

What I want to do is break down each common threat into five categories per step. First to understand and map out what defenses we need to systematically build, we need to know what the Malicious Action is.

After that we can move on to specific defensive mitigations for each of the actions identified, sometimes there will be more than one step involved. It might be a change in process, an added security feature that isn't being utilized, or possibly additional software or hardware.

My goal was to take everything and also assign a general ease of deployment to them. Creating a full matrix of what a defender may be able to focus on for some quick and easy wins down to some solutions that may take more planning and lots of money.

Not only should we worry about defending against each action, we should also implement correct monitoring and alerting. This will allow us to take reactive steps and aid in IR if the proactive ones have failed. Almost every defensive and monitoring step we cover today is FREE. No gimmicks or anything, just free settings that can be modified or added, or technologies implemented that are at no cost other than the time of the security or admin teams spend configuring them. A very under utilized tool included in most every enterprise organization is Group Policy. Since it's free and easy to walk everyone through, a handful of the demos will focus on changing settings there. We'll also show how the event viewer (and hopefully some sort of SIEM) will also play a part in detecting these use cases.

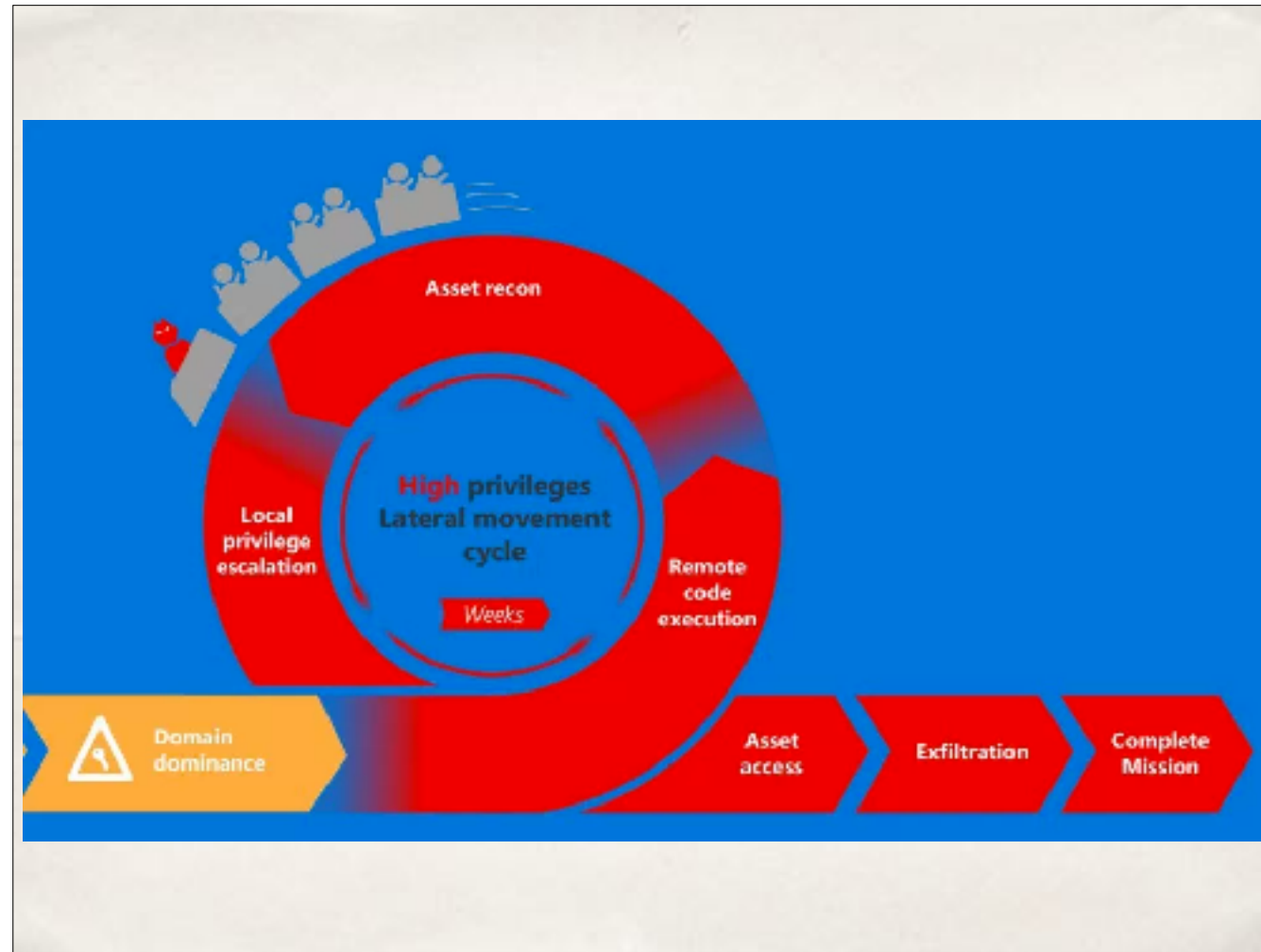
Talk about and show the spreadsheet <https://docs.google.com/spreadsheets/d/1J0swcA1Phb4mh-Pj8eR9ZEAlm5GEtz0UklP9YhVUbEY/edit#gid=0>



No two networks are the same right? Anyone that has been in more than one environment, whether it's blue or red team has never defended or attacked the exact same way twice. While this Kill...uh...roller coaster says months, we know that it could be anywhere from hours to months or years.

Include explanation about not everything fitting into threat model (lockheed martin)

<https://blogs.microsoft.com/microsoftsecure/2016/11/28/disrupting-the-kill-chain/>



The second loopdy loop from Microsoft is after a foothold has been gained and the attacker is in the network on the domain. It includes privilege escalation, code execution, and whatever the end goal might be.

There are lots of people that bash the kill chain, and rightfully so. There are so many different attack paths that it's hard to shoehorn them into any one type of thing. Even the two roller coasters from Microsoft aren't going to be able to cover each and every situation. But both are a good basis to see what does and doesn't fit, and use them to help craft a defensive strategy. And of course this model helps Microsoft, as they tie a handful of different technologies and services they provide to each step.



One major threat that I've wanted to cover is Ransomware. As we go through all 7 steps of the kill chain, not just with this example, but really with anything, it's the goal to continually make each additional action more difficult for the attacker. It's like a funnel, you stop as much as you can at the perimeter and work your way back. There are other methods that are also taking traction like zero-trust, which is a super cool concept. Just check out Beyond Corp and the design that Google and others have implemented to learn more about that.

Now over the course of these I'm going to be skipping some steps that aren't relevant and sometimes combining steps in the interest of not showing you 500 slides in the course of 3 hours. However I have all of this and more in the spreadsheet that I've just shown you and I'll release it publicly at the end of this tutorial. This spreadsheet is open for collaboration to the community so hopefully it will become a growing project that we can all benefit from.

Reconnaissance



Malicious Action

Defensive Mitigation
Ease of Deployment
Potential Monitoring
Detailed Alerting



So let's jump right in. I'll go through some explanation of certain sections, and we'll do a little over a dozen hands on walk throughs as well, maybe more if we end up having time.

First up is Reconnaissance. Even before any kind of attack or incident is happening, you should start prioritizing and taking action on what might happen. Risks Analysis, Business Impact Analysis, Threat Analysis.....all of these come into play when designing a defensive strategy. That's the whole basis of defensive security. But so many people stop at the basics, or hell, can't even handle the basics. Many people think that the first couple steps of the kill chain aren't worthy to defend against since it's out of your control. But when you start to break down each threat into the 7 steps you can see there are in fact steps you can take

Malicious Action

Attacker obtains email addresses, technologies used, and creates an organizational profile based on that information. OSINT for some companies is more difficult than others, but the more information that is out there the more in depth dossier an attacker can use to build phishing campaigns.

Here are a few examples from when I participated in the defcon SECTF. Attackers add this type of information to the profile for creating better targeted phishing.

Reconnaissance

Malicious Action



Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



At this point it's not really a defensive mitigation that we're concerned about, it's more of a defensive proactive measure.

Create policies around sharing internal information on sites such as LinkedIn or using corporate email addresses for nonbusiness use.

Go to : <https://canarytokens.org/generate>

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

 **Potential Monitoring**

Detailed Alerting



For Monitoring & Alerting there are a couple measures you can take to be proactive.

After a major breach has been seen on the news run a password reset. Even though they shouldn't, employees will reuse passwords for other services and sites.

Have corporate emails been seen in that breach or ones previously? How many emails are found with your own OSINT? (we'll cover this next)

Setup honey accounts! Do you control the design and content of any or all of your external facing websites or services? In this slide up here I have an embedded email address. An address that none of us can see, but guess who *can* see it? Bots and harvesters. Someone that is specifically targeting your website to scan for email addresses. You don't want your customers to see that email address and use it right? But it would be great as a honey account.

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

 **Detailed Alerting**

DEMO



One of my favorite tools I like to use to demonstrate a beginner level osint practice is using the harvester python script. Feel free to use this on your own domain if you want. Learning what is out there that attackers have access to is something that should be one of the steps you take as a defender.

Demo the harvester.py

Cd /usr/share/the harvester

Python Theharvester.py (use to show menu options)

Python the harvester.py -d [equifax.com](https://www.equifax.com) -l 50 -b all

Explain about using emails for internal campaigns

Delivery



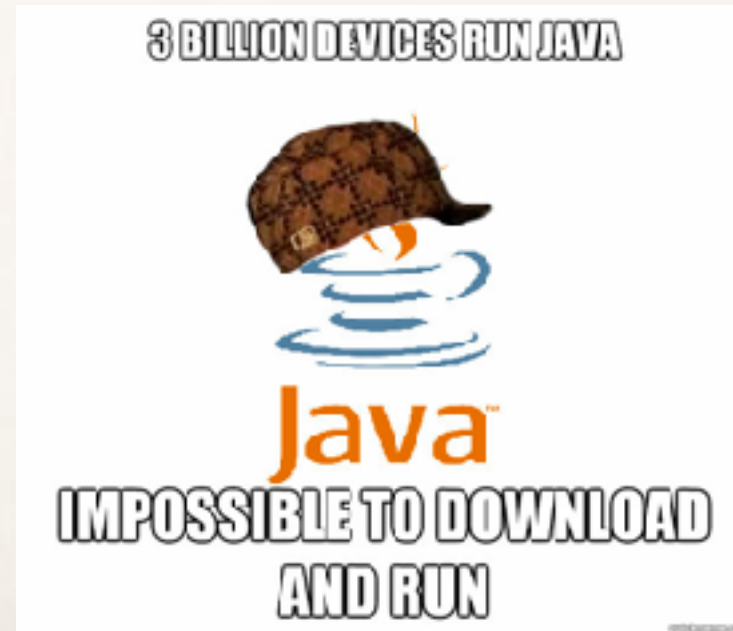
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Now we move on to the second step. As we all know most ransomware is distributed through means of phishing. If it's a targeted attack it will be based off of the information collected during the recon, or it could just be a mass mail.

Delivery

Malicious Action



Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO

.hta	HTML Scripting Application
.js	JavaScript
.jse	JavaScript Encoded
.pif	Program Information File
.scr	ScreenSaver
.wsf	Windows Script File
.wsh/.wsc	Windows Script Host
.vbe	Visual Basic Encoded
.vbf	Visual Basic File

There are several Defensive Mitigations that can be performed at this second step.

1. Assess which attachment types are needed in the organization. File types such as .js, .jse, .wsf, .wsh, .hta, .vbe, .vbf, .pif, .scr can be extremely harmful and are rarely exchanged from external sources. Block all from external sites or from being able to be opened at all. Of course there are legitimate uses for these filetypes, but there are ways around that.
2. Implement scanning on other attachment types for macros.
3. Implement mailing blacklists and greylists such as Spamhaus and dnsbl to block known malicious mail servers.
4. Instill the idea of "trust but verify" to your users. Correct user education is a key step in detection. The point of user education around this type of behavior has never been to make everyone experts in security, it has always been to arm the employees with basic knowledge so that in the event something out of the ordinary occurs, it may help notify the security team.
5. Implement Ad-Blocking

Group policy can be used to set the default application to notepad or something other than what is intended (java, word, etc) We can do this using the DISM tool (deployment image servicing and management) and group policy

1. Run an elevated command prompt on a machine that has your default application set correctly.
2. Type `dism /online /export-defaultappassociations:C:\Temp\defaultassociations.xml`. This creates an XML file that has all your file types and their current associations.
3. Edit the XML file to include only the file associations that you wish to enforce.

Now we'll go ahead and create a new GPO. Just to note as a best practice, leave the Default Domain Controller and Default Domain policies alone. Create a GPO from scratch and plan out control groups for the organization. Group policy can get super messy.

Delivery

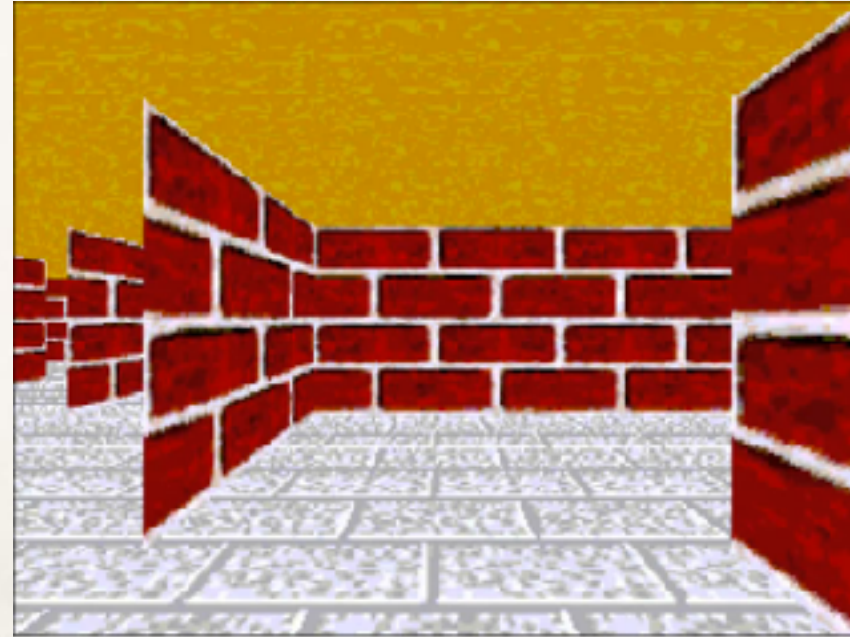
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

 **Detailed Alerting**



Filetypes of a certain size known to be malicious and associated with ransomware.

Flag .scr files over 22 MB and .js over 15 MB if you even let them in at all. Using mail attachment blocking is also an option.

Exploitation



Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



During the Exploitation phase, the endpoint downloads a JavaScript file, Microsoft Word, or document with malicious macro. These can either come from an attachment in the email itself or from a link that delivers a drive by download. As we've seen more recently there are techniques to spawn processes outside of an attachment without using macros, but at that point I hope you have an endpoint solution that realizes that a word document that runs powershell is a bad thing.

Exploitation

Malicious Action



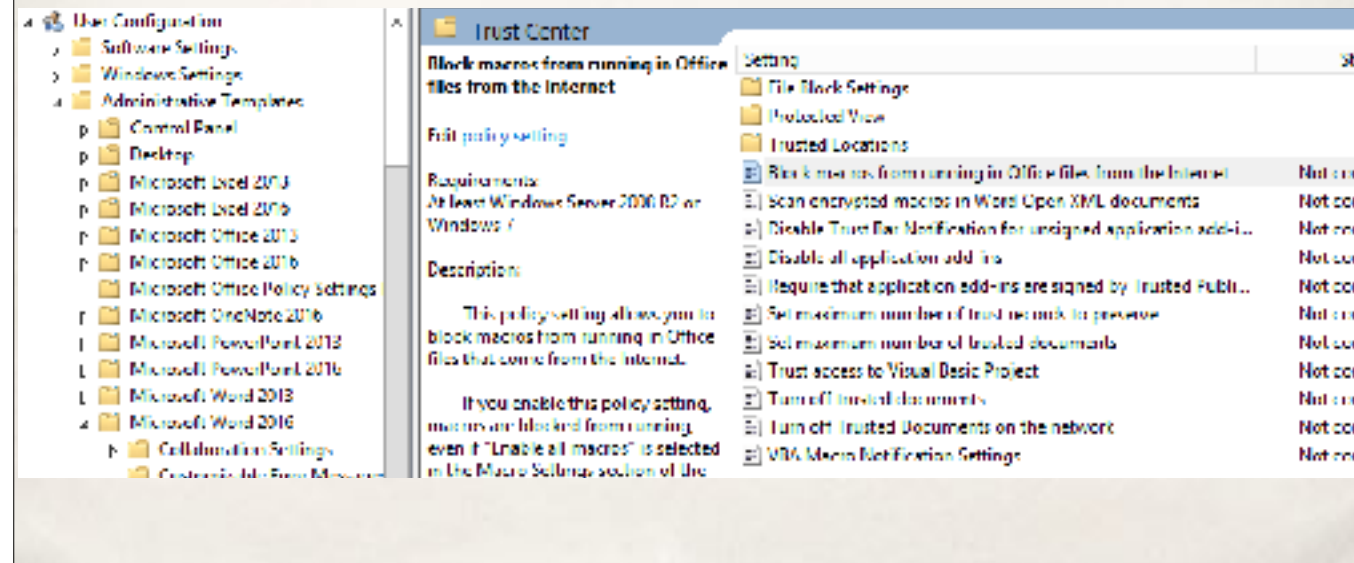
Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



1. Disable macros via group policy. And the great thing with doing it in group policy means you can still allow your admins and developers to run scripts as themselves, but not the majority of the users
2. Ensure any endpoint protection is up-to-date and installed. While a lot of people say Anti-virus is dead, I think it's still necessary. More recently there has been a shift to behavior based endpoint solutions as opposed to (or in addition to) signature based. Not only do many different compliance standards require it, it's still good at stopping the stuff that has been around for awhile and have signatures already.

You should have a windows DC server VM so we're going to go into that now and open up group policy editor

Gpedit.msc

You should also have the office admin templates for group policy, if not no worries, I'll go over it up here

Copy items in C:\temp\admx to c:\windows\policydefinitions and C:\temp\admx\en-US to c:\windows\policydefinitions\en-US

User Configuration\Admin Templates\Word\Word Options\Security\Trust Center\Block macros from running in Office files from the Internet

You can go even further with group nesting and group policy precedence to make sure only certain users have the ability to run macros if needed (hint: the majority of them don't)

There are so many other security settings that you can make use of in here as well, however you'll want to make sure enabling them isn't going to effect any end user's ability to do their job. For example, if you have one or two application add-ins, see if you can get the publishers to sign them.

Exploitation

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

```
char *decode(char *s, size_t len) {  
    for (int i = 0; i < len; i++)  
        s[i] ^= 0x15;  
    return s;  
}  
  
int main(int argc, char *argv[]) {  
    struct hostent *addr =  
        gethostbyname(decode(")aaef/::lz`a`;wp:qDb!b,BrMvD", 28));  
    return 0;  
}
```

Monitor proxy logs for unexpected file retrievals (e.g., JavaScript is the first file fetched from that host, host is on a threat intel list, etc.)

Use proxies or IDS (if cleartext) to monitor for known de-ob-fus-cation strings that malware uses to attempt to hide parts of their binaries.

Shown above is FLOSS from Fireeye Labs. It offers the ability to deobfuscate them for use in any incident response procedures you may perform internally.

Installation



Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Unless any of you feel like infecting yourselves with ransomware, we'll gloss over the malicious installation. The payload is executed on the end user's device. Keep in mind ransomware variants like Lucky, Cerber, CryptoWall, and others will use the built-in Windows Cypto API to handle the encryption.

Installation

Malicious Action



Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Defensive Mitigation

1. Keep backups (that are not permanently attached) so that encrypted files can be restored easily. You should have a full DR and backup plan that takes into account RPO (recovery point objective) and RTO (recovery time objective) for all business critical data.
2. Depending on OS, you can use "filesystem firewalls" to permit access to files on per-process basis. That means that you can permit read access to MS Word, but not IE, for example.
3. There are experimental techniques that can be used to block crypto-based ransomware (e.g., Decryptonite) <https://github.com/DecryptoniteTeam/Decryptonite>
4. Have a portion of your IR procedure set aside to document at what point it's worth it to either pay the ransomware (which should always be a last resort) or just wipe the drive. Not everyone has the staff or budget for a full IR investigation. Part of that procedure could include making use of an already in place contract of a third party. And make sure it's an agreement that is already in place. Calling at the last minute for an incident to a company that you don't already have a relationship with may end up costing a lot more money.

Installation

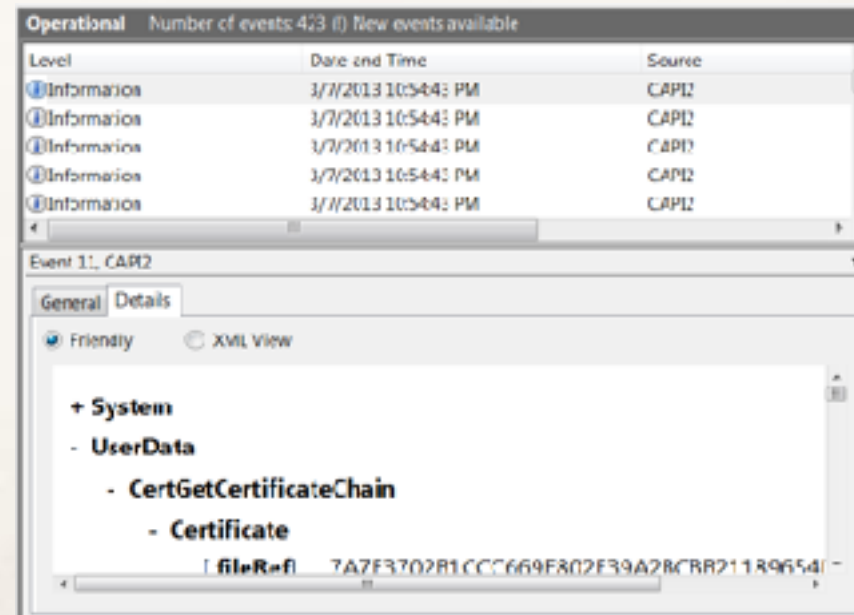
Malicious Action

Defensive Mitigation

Ease of Deployment

 **Potential Monitoring**

Detailed Alerting



Monitoring & Alerting

Like we covered a second ago, High increase in Windows Crypto API over short amount of time may be triggered by certain strains of ransomware encrypting the file system.

Command & Control

🦠 Malicious Action

Defensive Mitigation
Ease of Deployment
Potential Monitoring
Detailed Alerting



The ransomware contacts a C&C server on the internet to transmit the decryption key.

Command & Control

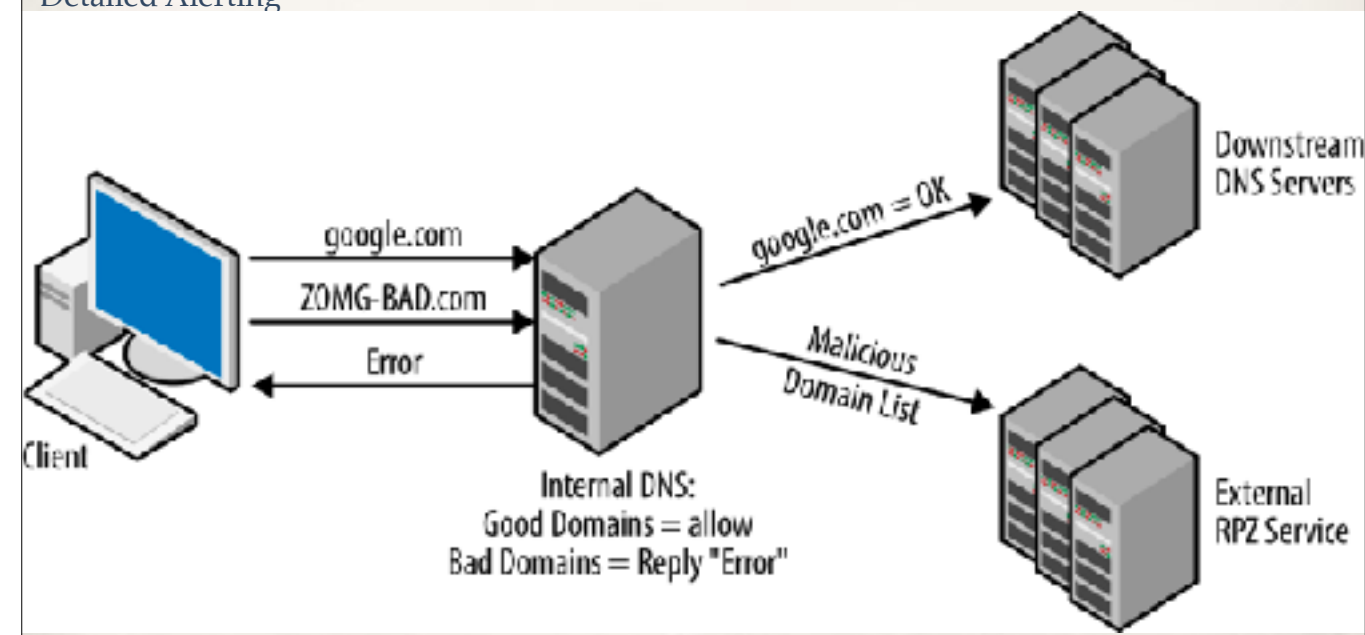
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



This is a simple diagram showing how DNS sinkholes work. If you implement sinkhole DNS you can autoblock outbound connections to known malicious IP addresses. Not only can you pull in information from other services on what domains to block, but you can also use the information from your own internal IR procedures to add information to them as well. For example*****talk about phishing campaign at FRMC..

Command & Control

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

THREAT FEEDS			
BOTS	MALWARE	OTHERS	PORT SCANNERS
botch C&C server	Malwaredomains1	CI Army List	Port 110 Scanner
Crystalwall C&C server	Malwaredomains	Emergingthreats	Port 143 Scanner
Cynara Servers	Threatspdr	Forum Spammers	Port 81 Scanner
Eosporbot C&C server		Male0de Backlist	Port 22 Scanner
mstisu C&C server		TLD Name Servers	Port 25 Scanner
Pakvo C&C IP		Tor Exit Node ✓	Port 443 Scanner
qakbot C&C server			Port 60 Scanner
ramnit C&C server			Port 662 Scanner
Farsomdomains			Apache Web Server Scanner
Farsomua			Asterisk VoIP Scanner
Gaysys C&C server			Guaped Bot/Tricked
Symmi C&C server			Buteforce
TinyBanker C&C server			courier imap attacker
Upatr Servers			courier pop3 attacker
Webh0n.Bots			OpenBL FTP Scanners
Zeus C&C server			Upats HTTP Scanners
Zeus C&C server			OpenBL MAIL Scanners
			OpenBL SMTP Scanners
			OpenBL SSH Scanners

Threat lists or threat intel should never be blindly accepted, implemented, or monitored. The wealth of information that is out there on any threat topic is staggering. But in truth it all comes down to how you use what information for your specific threats in. Your specific environment. There are known C&C servers on threat lists that can be used in DNS sinkholes. There is this section on SANS https://isc.sans.edu/suspicious_domains.html that also will break down the threat feed into different levels of severity and <https://isc.sans.edu/threatfeed.html>

Connection to known C&C servers. (part of a threat list that could be beneficial)

Command & Control

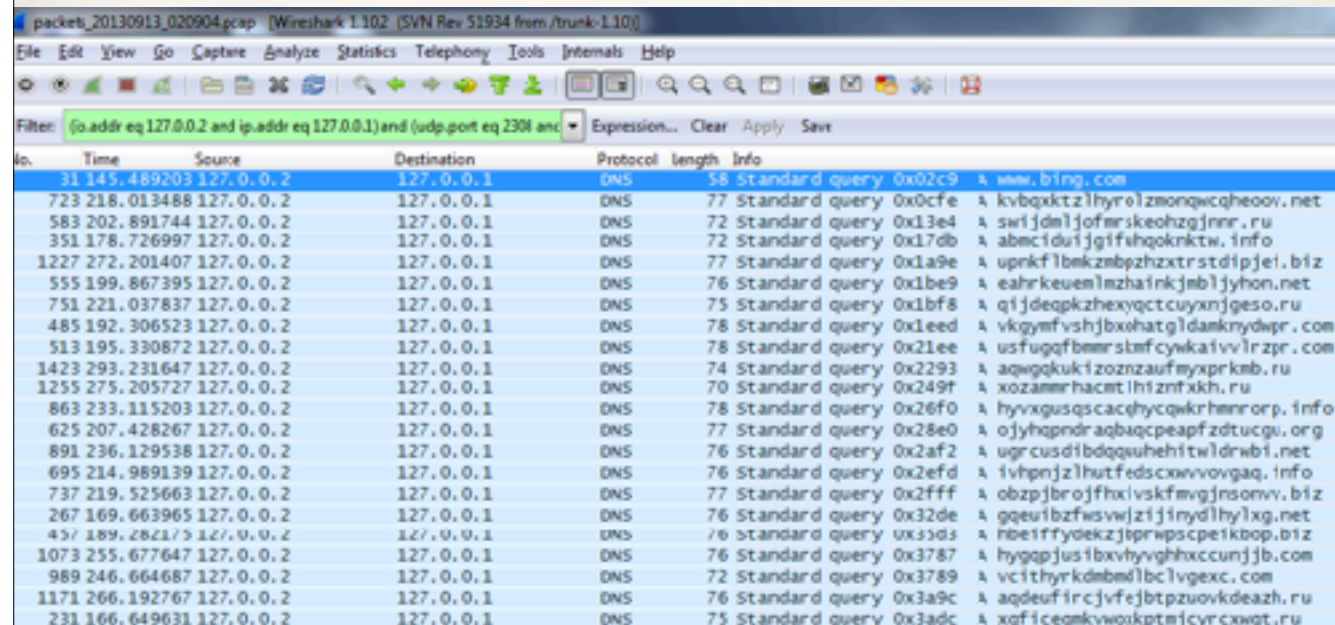
Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



The image shows a Wireshark packet capture of DNS traffic. The filter is set to '(ip.addr eq 127.0.0.2 and ip.addr eq 127.0.0.1) and (udp.port eq 2304 and ...)'. The packet list shows 23 packets, all of which are DNS standard queries from 127.0.0.2 to 127.0.0.1. The packet details pane shows the first packet, a standard query for 'www.bing.com'.

No.	Time	Source	Destination	Protocol	Length	Info
31	145.489203	127.0.0.2	127.0.0.1	DNS	58	Standard query 0x02c9 A www.bing.com
723	218.013488	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x0cfe A kvbqxktzlhylzmonqwcqheooov.net
583	202.891744	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x13e4 A swijdm1jofmrskeshzgjnnr.ru
351	178.726997	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x17db A abmciduijgishqoknktw.info
1227	272.201407	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x1a9e A upnkflbmkbzbpzhztrstdipjei.biz
555	199.867395	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x1be9 A eahrkeuennlmzhaikjmblijhon.net
751	221.037837	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x1bf8 A qijdeqpkzhexyqctcuyxnjgeso.ru
485	192.306523	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x1eed A vkgyfvsjhjbxhatgldamknydwpr.com
513	195.330872	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x21ee A usfugqfbemrslmfcywkaivvlrzipr.com
1423	293.231647	127.0.0.2	127.0.0.1	DNS	74	Standard query 0x2293 A aqwgqkukizoznauzafmyxprkmb.ru
1255	275.205727	127.0.0.2	127.0.0.1	DNS	70	Standard query 0x249f A xozammrhacmtlhizntxkh.ru
863	233.115203	127.0.0.2	127.0.0.1	DNS	78	Standard query 0x26f0 A hyvxgusqscacqhyqcwkrhmrorp.info
625	207.428267	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x28e0 A ozyhqndraqbaqqceapfzdtucgu.org
891	236.129538	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2af2 A ugrcusdibdqquhehitwldrwbj.net
695	214.989139	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x2efd A ivhpnjzlhutfedscxovvovgaq.info
737	219.525663	127.0.0.2	127.0.0.1	DNS	77	Standard query 0x2fff A obzpjbrojfhxivskfmgjnsomv.biz
267	169.663965	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x32de A ggeuibzfwavwjzjinydlhylxg.net
457	189.282175	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x33d3 A nbeiffrydekzjbrwpsceikbop.biz
1073	255.677647	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3787 A hygqjjustibxvhyvghhxcunjjb.com
989	246.664687	127.0.0.2	127.0.0.1	DNS	72	Standard query 0x3789 A vcithyrkdbmblbclvgexc.com
1171	266.192767	127.0.0.2	127.0.0.1	DNS	76	Standard query 0x3a9c A aqdeufircjvfejbtpzuovkdeazh.ru
231	166.649631	127.0.0.2	127.0.0.1	DNS	75	Standard query 0x3adc A xqficeomkvwookptmfcvrcxwqt.ru

Excessive numbers in a domain or low % of meaningful strings or dictionary words in domain could point to the ransomware reaching out to the Command and Control server using a Domain Generation Algorithm or DGA. There are a few IPS solutions that have algorithms to detect and block domains that fall within these categories. The DGA technique is in use because malware that depends on a fixed domain or IP address is quickly blocked, which then hinders operations. So, rather than bringing out a new version of the malware or setting everything up again at a new server, the malware switches to a new domain at regular intervals.

Action & Objectives

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Volume Shadow Copy Deletion

The malware starts encrypting the files on the hard disk, mapped network drives, and USB devices. Once completed, a splash screen, desktop image, website, or text file appear with instructions for the ransom.

Action & Objectives

Malicious Action



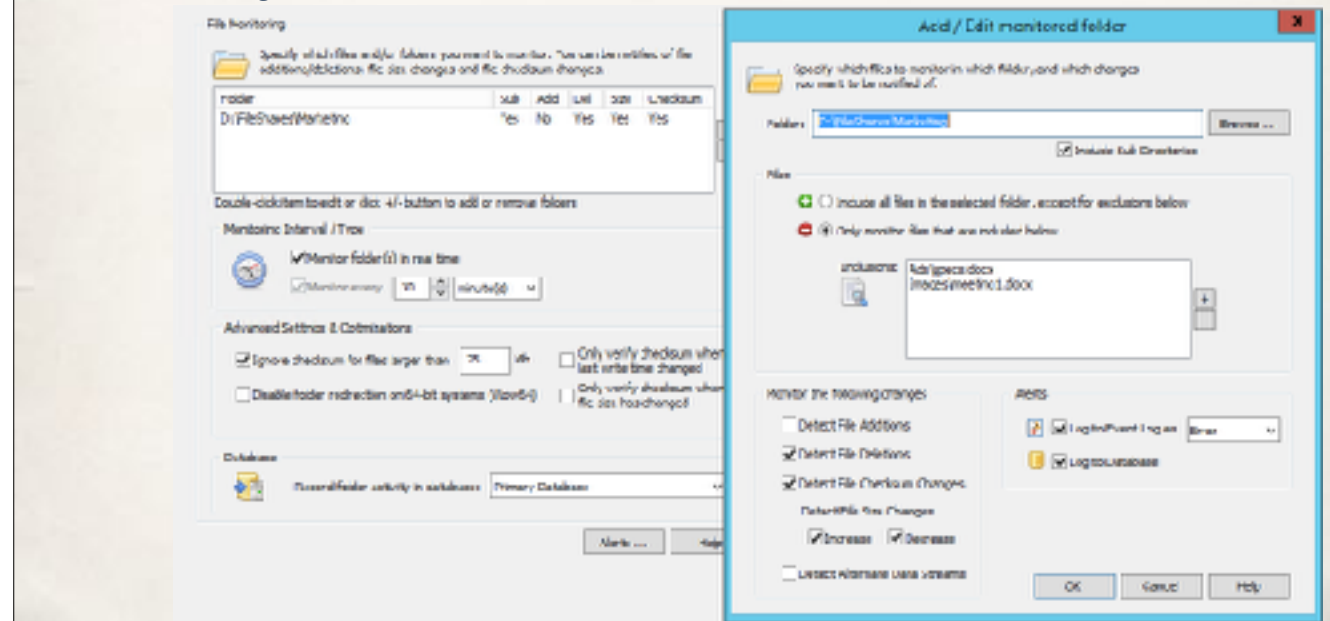
Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



Implement Honey Directories—the ransomware goes into C:\\$\$ it sees another \$\$ directory, when it goes into C:\\$\$\\$\$ it sees another \$\$ directory, and so on. (you can do the same sort of thing using windows FSRM-file server resource manager- <https://blog.netwrix.com/2016/04/11/ransomware-protection-using-fsrm-and-powershell/>)

What the team at Free Forensics did was use a PowerShell script to create a mount point in the root of the C:\ volume. They labelled that mount point \$\$, and when ransomware hits that mount point it starts following a loop. The PowerShell script makes recursive directories inside the original directory, so when the ransomware goes into C:\\$\$ it sees another \$\$ directory, when it goes into C:\\$\$\\$\$ it sees another \$\$ directory, and so on, up to a maximum path size of 256 characters (this is a Microsoft limit).

Unlike filenames, where it is hard to be sure which file will be read first by the ransomware, directories are enumerated and processed alphabetically, which is why the files in C:\\$Recycle.Bin are usually encrypted first. Which means this can serve as an early warning system.

1. Run powershell script to create C:\\$\$
2. Computer>windows settings>security settings>Advanced Audit>Object Access>Audit File System> enable success
3. ON the C:\\$\$ folder..... right click, properties, security, advanced, auditing, everyone/success
4. Event viewer, security, eventID 4656 with object name = C:\\$\$

For more advanced options you can use a service like tripwire, afick (another file integrity checker)

<http://www.freeforensics.org/2016/03/proactively-reacting-to-ransomware.html>

Action & Objectives

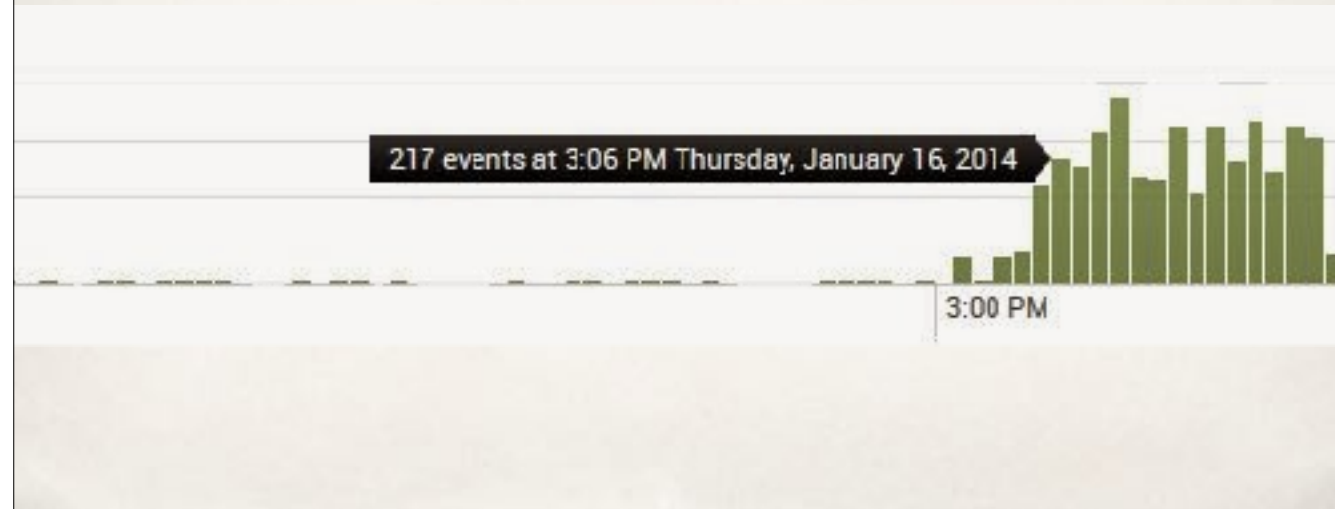
Malicious Action

Defensive Mitigation

Ease of Deployment

 **Potential Monitoring**

Detailed Alerting



53

Advanced file auditing can be enabled for alerting on an extreme increase in filesystem changes.

They also have Windows Logging Cheatsheet and other cheatsheets for what is and isn't helpful to capture in logging in relation to security
<http://hackerhurricane.blogspot.com/>

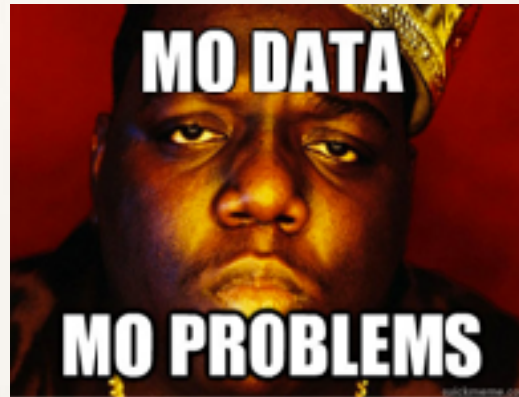
break/questions - 15 minutes

Theft, Loss, & Data Exfiltration

Theft, Loss, & Data Exfiltration is something that many organizations attempt to defend against by implementing DLP or Data Loss Protection. Even if Data Exfil isn't malicious, we'll end up skipping the second and third steps (Weaponization/Delivery) of the kill chain. This is another one of those cases that it could be an advanced attack, but by originating from the inside of the network the attacker already has the advantage.

A DLP solution would be a perfect addition to the defensive mitigations we'll end up covering. First a little primer on DLP and some best practices prior to implementing a solution

The Notorious DLP



No DLP solution is going to keep your data 100% safe. Almost everyone has a smartphone and can screenshot with very little chance of detection or send data via chat in any number of communication programs (Skype, Google Hangouts, etc). Short of having a SCIF (Sensitive Compartmented Information Facility) the focus for most DLP programs will be on protecting against the loss of larger amounts of data and honest accidents.

3 areas of DLP to remember

1. Endpoint protection - Some endpoint solutions like Symantec already contain DLP options, other solutions come with their own endpoint clients with additional features.
2. Network protection - Network traffic monitoring can enhance visibility into data in motion and flowing between segments, organizations, or leaving the enterprise.
3. Physical - Any solution should also include proper planning for physical copies of data as well. Printed copies, hard drives, or other equipment that aren't secured can also be a high risk that shouldn't be forgotten.

Data Classification

—5 steps—

- Identify Sources
- Information Classes
- Map Protections
- Classify & Protect
- Repeat

1. Identify data sources to be protected.

Completion of this step should produce a high-level description of data sources, where it resides, existing protection measures, data owners and custodians, and the type of resource. Obtaining this information can be difficult, but can be an added part of the documentation process as data owners and custodians are assigned and documented. There are software solutions specifically created for e-discovery of data at rest in an organization.

2. Identify information classes.

Information class labels should convey the protection goals being addressed. Classification labels like Critical and Sensitive have different meanings to different people, so it is important that high-level class descriptions and associated protection measures are meaningful and well-defined to the individuals who will be classifying the information as well as those who will be protecting it and using it.

3. Map protections to set information classification levels.

Security controls such as differing levels and methods of authentication, air-gapped networks, firewalls/ ACLs, and encryption are some of the protections involved in this mapping.

4. Classify and protect information.

All information that has been identified in step 1 should now be classified as dictated in step 2, and protected as in step 3.

5. Repeat as a necessary part of a yearly audit.

Data footprints are ever expanding. New software is installed or upgraded with add-ons and now data has grown or changed in scope. A yearly audit of the current data footprint in the enterprise will be required to ensure data continues to be protected as documented.

Map Data —3 Types—

Data at Rest

Data in Motion

Data in Use

You can't protect data if you don't know where it resides or how it moves throughout the organization. Knowing where the sensitive data is and how it is structured will go a long way in ensuring the correctly formatted rules are in place.

1. Data at Rest: Data in databases, on file servers, or in custom applications not only should be identified as previously stated, but also encrypted and in a secure physical location.
2. Data in Motion: Common avenues of data access to pay attention to (and their ports) are FTP (21), SFTP(22), SMTP(25), HTTP/APIs(443/80/8080), SMB(445). Any network monitoring solution should be able to alert on sensitive data in transit.
3. Data in Use: Data that can be exfiltrated using things like CDs, USB drives, or with copy/paste to external websites from the user endpoints. A comprehensive DLP solution should have the ability to analyze data before it is transferred to removable media, and automatically encrypt sensitive information as it is stored on the removable media. It should also prevent data from being printed, faxed, or copied into memory to paste to another document

Implementation

Any type of DLP deployment should be thoroughly tested in a smaller more controlled implementation before being introduced to the larger enterprise. Begin with simple rules in monitor mode that will allow you to observe what will eventually be allowed, blocked, or alerted on. This period gives the ability to modify strategy and fine tune rules for a smoother roll out on a larger scale.

Don't just assume that the initial roll out of a DLP solution is working and will continue to work. Reassessments, testing of controls, and change processes should also occur on a regular basis. Just like the majority of security implementations it will not be a one time project, but a process that continues to grow and be shaped by the type of data the organization holds. Add to regular penetration tests a section where DLP is tested from an offensive viewpoint.

Reconnaissance



Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Now that we've covered an overview of the Loss portion of this use case, I'm going to focus more on malicious exfiltration by either an employee or an outsider.

There are several ways of handling recon work for the purpose of exfiltrating data.

1. Port scanning
2. Scanning for open file shares
3. Testing for default or weak credentials
4. Active Directory queries
5. Wifi sniffing

Most data requires at least some sort of authentication to access, other than completely open fileshares or anonymous ftp

Reconnaissance

Malicious Action



Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

```
node "c2950.domain.com" {  
  
    Interface {  
        duplex => auto,  
        speed => auto  
    }  
  
    interface {  
        "FastEthernet 0/1":  
            description => "--> to end-user workstation",  
            mode => access,  
            native_vlan => 1000  
    }  
}
```

If we focus on malicious attempts and not end users losing the data on accident there are a fair amount of defensive measures we can take to prevent certain types of recon.

1. Disable unused ports by using puppet (shown), rancid, net disco
2. Auto-shun port and vuln scans from all external entities. <https://www.autoshun.org/> (and other hosting providers) Because we don't want to alert on port/vuln scanning from the outside!
3. Disable open shares or IP Address restrict open shares with endpoint firewalls

Reconnaissance

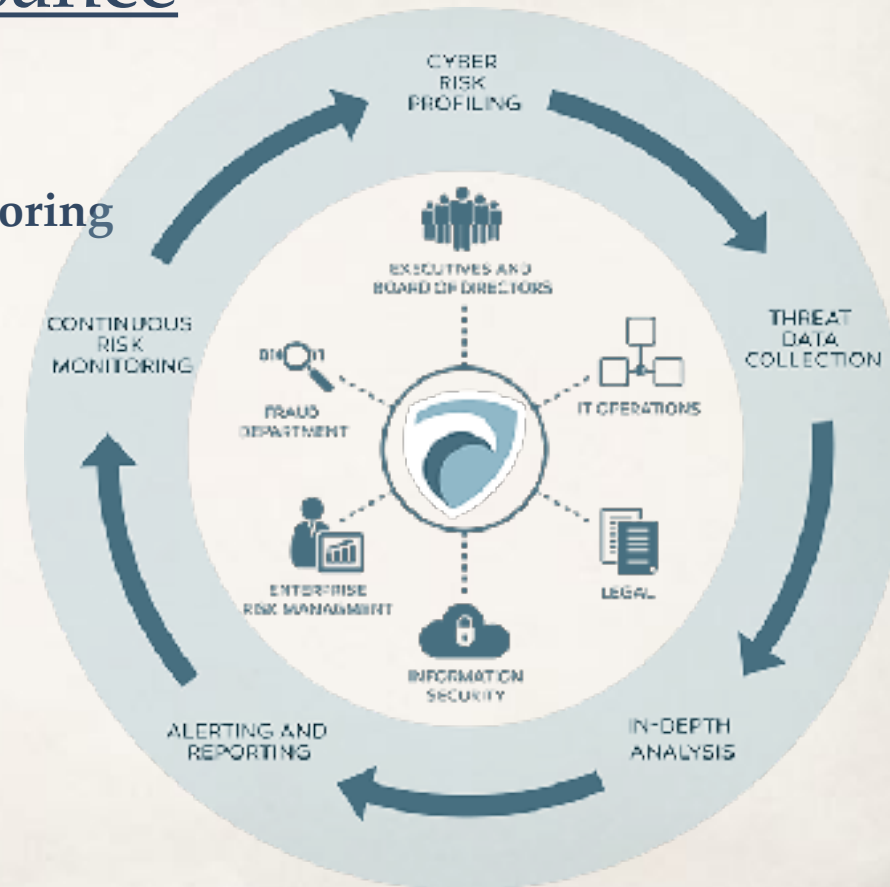
Malicious Action

Defensive Mitigation

Ease of Deployment

 **Potential Monitoring**

Detailed Alerting



At a minimum, this is what it takes to implement threat detection. Many times organizations use threat lists. I've mentioned them before as something that can be added to the firewall to automatically block with. However, there is so much more to threat lists than slapping them into a monitoring or alerting system. Please please **Do not** alert on threat list activity! ** Explain why**

Reconnaissance

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring



Detailed Alerting

1. Alert on session querying/command history??

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing>

And

Query.exe (4688) seems to be what shows up for “session query”

Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Detailed Tracking> Audit Process Creation

Computer Configuration > Administrative Templates\System\Audit Process Creation\Include command line in process creation events

When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings.

Computer Configuration>Policies> Windows Settings>Security Settings>local Policies>Security Options>Audit: Force audit policy subcategory settings

Exploitation



Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



MFA/2FA is Bypassed on Successful Authentication - talk about how some 2FA is implemented incorrectly

Net Use command to mount remote root share - monitor for net use?? Kind of sucks with mapped drives?? Maybe not after boot/logon?

Anomalous Access to Externally facing server is obtained

Exploitation

Malicious Action



Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Deploying MFA/2FA, which we've already covered is one of the better defensive mitigations. Others include WAF, Proxies, DMZ, a well structured, segmented and designed network. I've heard time and time again that pentesters are stopped by 2fa being implemented internally.

Installation

🦹‍♂️ Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



FTP or other file transfer software may be installed. DNS Tunneling programs can also be used like DNScat or iodine and can be incredibly effective. Many of the tools for creating DNS tunnels were created with the intent of bypassing captive portals for paid Wi-Fi service as well as bypassing MFA. If one of these systems allows all DNS traffic out, a DNS tunnel can be set up to tunnel IP traffic without paying for service and bypassing any type of monitoring or control.

Installation

Malicious Action



Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Application whitelisting, egress filtering, anomaly detection. You should know what devices are allowed to perform external DNS queries as well as what that DNS traffic looks like. Egress filtering will stop unauthorized endpoints from accessing the internet on ports other than the ones you allow. Not just egress filtering per say, but remember least access is preferred.

Installation

Malicious Action

Defensive Mitigation

Ease of Deployment



Potential Monitoring

Detailed Alerting



Many of the DNS tunneling utilities do not try to be stealthy. They are relying on the fact that DNS is often not monitored. There's a great SANS white paper on detecting DNS exfil anomalies that goes into better details on what to monitor. Things like the size of the request and response, statistical analysis, and hosts using uncommon record types or attempting DNS resolution to the internet as opposed to the internal enterprise solution.

Action & Objectives

Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

 **Detailed Alerting**

DEMO



I just have to say I love this picture for the sheer craziness of it.

One of the top worries of data exfiltration with companies is that the information may end up on the dark web somewhere. While the majority of the time data exfil won't go directly to TOR from the compromised network, it's still helpful to monitor for.

Demo capturing TOR traffic with IDS??

Snort -D -de -l /var/log/snort -c /etc/snort/snort.conf

Go over conf

Config checksum: none

Lateral Movement & Privilege Misuse

Reconnaissance



Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



Certain things in the reconnaissance phase that attackers are more likely to use are

Testing of default or weak credentials

Using bloodhound to enumerate users in Active Directory

Use of pre-installed tools and commands to gather intel on internal systems

And a few things that can be super noisy, but still happen are

Internal Port Scanning and Internal Vulnerability scanning

Bloodhound will allow pretty much anyone to enumerate the active directory database. So we're going to go through how to detect its use as long as you're logging on the device that it's being run from. Bloodhound also has a database connection that they have walkthroughs on, that will show graphs of the AD enumeration, but we don't really have to worry about that as that takes a significant time to setup and test.

If you've never used powershell before, there's this thing called the execution policy, that would prevent us from running powershell scripts. There are ways that attackers get passed the execution policy, but since we're domain admin's on our own DC, we can just change it ourselves.

1. Get-ExecutionPolicy will show you what it is currently set at
2. Set-executionpolicy unrestricted to change it and allow us to run bloodhound

1. Cd C:\temp\BloodHound-master\BloodHound-master\PowerShell
2. Import-Module .\Bloodhound.ps1

Reconnaissance

Malicious Action



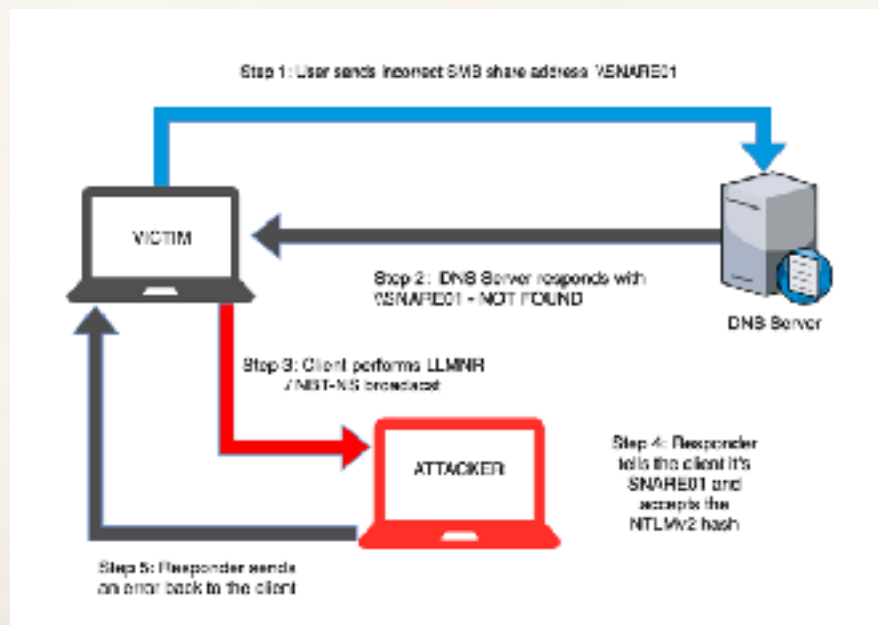
Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



One of the first methods of attack that can be performed is using Responder by SpiderLabs. This tool allows the spoofing of LLMNR and NBT-NS responses to queries that Windows workstations broadcast by default on a network. By default, when a Windows workstation requests a name lookup, it performs the following three queries: Local Hosts File, Configured DNS Servers, and NetBIOS Broadcasts. If the first two queries return no results, the machine broadcasts an NBT-NS request, of which any device on the network would be able to respond to. LLMNR queries are made after a DNS query fails to see if the device in question is on the local network. By using Responder you can answer these requests and possibly gain usernames and password hashes.

Disable LLMNR

1. Open gpedit.msc
2. Goto Computer Configuration -> Administrative Templates -> Network -> DNS Client
3. Click on "Turn Off Multicast Name Resolution" and set it to "Enabled"

You can't really disable netbios directly within group policy, but there are a few different ways that you can get it done. There is a powershell script here

Disable NetBios

Via powershell(<https://www.alexandreviot.net/2014/10/09/powershell-disable-netbios-interface/>):

```
$adapters=(gwmi win32_networkadapterconfiguration )
```

```
Foreach ($adapter in $adapters){
```

```
    Write-Host $adapter
```

```
    $adapter.settcpipnetbios(2)
```

```
}
```

OR

```
set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces\tcpip* -Name NetbiosOptions -Value 2
```

Reconnaissance

Malicious Action



Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO

8 characters at only lowercase equals 26^8 . Extremely easy, will crack in < 2 minutes.	baseball
8 characters at upper- and lowercase equals 52^8 . Still not the best, will crack in < 6 hours.	Baseball
8 characters at uppercase, lowercase, and numbers equals 62^8 . A little better, will crack in < 24 hours.	Bas3ball
10-character passphrase with uppercase, lowercase, numbers, and symbols 94^{10} . Approximately 600 years.	Base64b@ll

Because there is such a large amount of defensive things to cover, this one gets a second slide!

Here are some ballpark statistics on time to crack certain password complexities. One of the larger hurdles in organizations are what should the complexity requirements be? Too short isn't secure, but too long and complex and the users start writing things down.

Well good news, in Windows Server 2008 Microsoft introduced the capability to implement fine-grained password policies (FGPP). Using FGPP can be extremely beneficial to control more advanced and detailed password strength options. There are some cases when certain users or groups will require different password restrictions and options, which can be accomplished by employing them.

Encourage password managers and implement 2FA internally.

PSO??

([https://msdn.microsoft.com/en-us/library/windows/desktop/ms721766\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms721766(v=vs.85).aspx))

1. go to "Turn Windows Features On or Off" and make sure the "AD DS and AD LDS Tools"
2. Under Administrator Tools, open ADSI Edit and connect it to a domain
3. Double-click the "CN=DomainName", then double-click "CN=Password Settings Container",
4. right-click "CN=Password Settings Container". Click "New" and then "Object...".
5. Give it a name
6. Set ms.DS-PasswordSettingsPrecedence to "10." This is used if users have multiple Password Settings Object (PSO) applied to them.
7. Set msDS-PasswordReversibleEncryptionEnabled to "FALSE."
8. Set msDS-PasswordHistoryLength to 24 This will be the number of passwords that are remembered and not able to be reused.
9. msDS-PasswordComplexityEnabled to TRUE.

Reconnaissance

Malicious Action

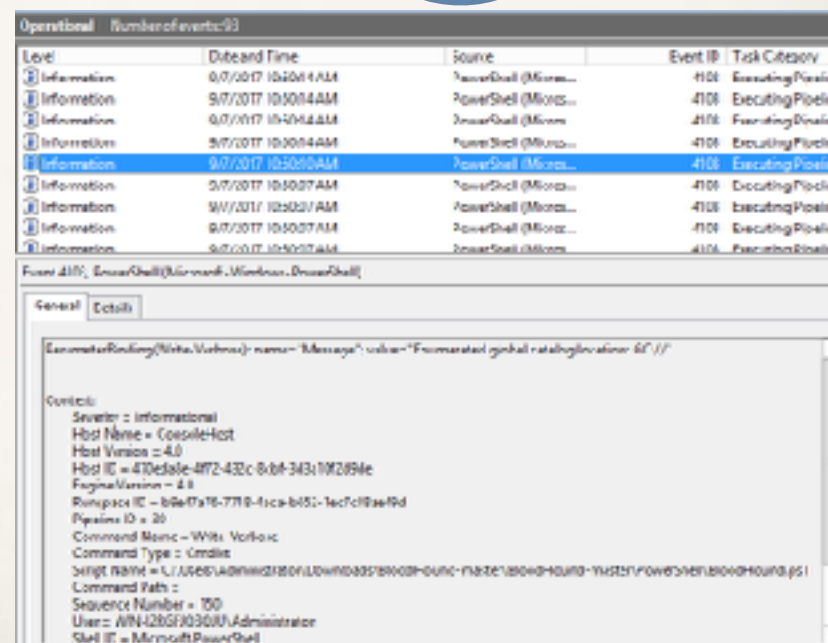
Defensive Mitigation

Ease of Deployment

Potential Monitoring

 **Detailed Alerting**

DEMO



Level	Date and Time	Source	Event ID	Task Category
Information	9/7/2017 10:00:04 AM	PowerShell (Micro...	4103	Executing Pipeline
Information	9/7/2017 10:00:04 AM	PowerShell (Micro...	4103	Executing Pipeline
Information	9/7/2017 10:00:04 AM	PowerShell (Micro...	4103	Executing Pipeline
Information	9/7/2017 10:00:04 AM	PowerShell (Micro...	4103	Executing Pipeline
Information	9/7/2017 10:00:07 AM	PowerShell (Micro...	4103	Executing Pipeline
Information	9/7/2017 10:00:07 AM	PowerShell (Micro...	4103	Executing Pipeline
Information	9/7/2017 10:00:07 AM	PowerShell (Micro...	4103	Executing Pipeline
Information	9/7/2017 10:00:07 AM	PowerShell (Micro...	4103	Executing Pipeline

Event ID: 4103, PowerShell (Microsoft Windows PowerShell)

General Details

Source: Microsoft Windows PowerShell

Category: Informational

Host Name: Coepile-Host

Host Version: 4.0

Host ID: 4103-4103-4103-4103-4103-4103-4103-4103

Process Name: powershell.exe

Process ID: 20

Command Name: powershell.exe

Command Type: Cmdlet

Script Name: C:\Users\Administrator\AppData\Local\Microsoft\Windows\PowerShell\PowerShell\Modules\Bloodhound\Bloodhound.ps1

Command Path: C:\Users\Administrator\AppData\Local\Microsoft\Windows\PowerShell\PowerShell\Modules\Bloodhound\Bloodhound.ps1

Sequence Number: 100

User: NT AUTHORITY\SYSTEM

Shell ID: Microsoft PowerShell

Now we come back to alerting on the Bloodhound demo I showed a minute ago.

First we need to enable advanced powershell logging - User>Admin Templates>Windows Components>Windows PowerShell....enable and set module names to *

1. Cd C:\temp\BloodHound-master\BloodHound-master\PowerShell
2. Import-Module .\Bloodhound.ps1
3. Invoke-Bloodhound

You can see in Event Viewer where it's enumerating the global catalog Event ID 4103 now that advanced powershell logging is enabled. You can also use this to your advantage to alert on powershell commands that exceed a certain length or have other common attack or recon switches being run, especially by non-trusted users.

WMI, Powershell, vbscript, or ntdsutil commands from unauthorized user/host:

Event ID : 1 (Process Create)

5 (Process Terminated)

- Image : "C:\Windows\System32\wbem\WMIC.exe"

OR

- Image : "C:\Windows\System32\Windows PowerShell\v1.0\powershell.exe"

OR

- Image : "C:\Windows\System32\cmd.exe"

OR

- Image : "C:\Windows\System32\ntdsutil.exe"

Weaponization



Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



The most common and helpful thing you can do to prevent malicious actions at this stage is to implement application whitelisting. There are so many harmful tools out there, even a handful that already come with windows, that aren't needed on every system or needed by every user. I'm sure many of you know, but black listing applications has proven not to work. It's the security equivalent of using your fingers to stop water from leaking out of a holy bucket

Exploitation



Malicious Action

Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting



Exploitation is where all the action happens. Mimikatz, pass the hash, sticky keys, credentials being extracted from memory and golden tickets all fall into this step. We're talking about lateral movement, so this is a big chunk of the activities we need to try and defend against.

Exploitation

Malicious Action



Defensive Mitigation

Ease of Deployment

Potential Monitoring

Detailed Alerting

DEMO



The primary defense against mimikatz (and other privilege escalation) is limiting administrative privileges to only those users that need it. I know that it's easier said than done. I'm sure a very very small percentage of us have had the ability to build an environment from the ground up. Usually you are slapped into a network that was built without design or security in mind, and I'm sure least privilege wasn't a consideration when a piece of software or business function just needed to work.

A couple other things that you can look into are

Enabling SMB Signing

Privilege Access Workstations (PAWs or Jumpboxes)

Protected Accounts in AD 2012R2 and above

The two methods we'll walk through real quick are LAPS (Local Admin Password Solution) and Enabling the Local Account Token Filter Policy, which prevents non-interactive logins for local admins. This second one could be extremely difficult depending on the environment. You would have to have other methods in place for managing endpoints as it will break WMI.

DEMO

1. Run laps exe
2. Create laps gpo
3. Create share with .msi file for domain users and COMPUTERS
4. Computer Configuration > Policies > Software Settings. Right click on Software Installation and click New > Package. = \\TEST-DC\LAPS-Share
5. Gpupdate /force on client machine
6. Extend Schema

Testing & Proof of Concept

So now what? Time to create some drills and tabletop exercises! A tabletop exercise is a meeting of key stakeholders and staff that walk step by step through the mitigation of some type of disaster, malfunction, attack, or other emergency in a low stress situation. A drill is when staff carries out as many of the processes, procedures, and mitigations that would be performed during one of the emergencies as possible.

What are a few things that you can use to come up with these scenarios? (real IR, pentests, new threats for other companies)



While drills are limited in scope, they can be very useful to test specific controls for gaps and possible improvements. A disaster recovery plan can be carried out to some length, backups can be tested with the restoration of files, and services can be failed over to secondary cluster members.

Any of the stuff we walked through over the last 3 hours.....implement it and test it! This is exactly what purple teaming is. Whether you have an internal red team or it's just you. Test to make sure the defensive tactics that you have in place are working how they should be, and see if you can get around them. Maybe that TOR rule doesn't take into account if you are attached to the wifi, or maybe one of your SIEM rules doesn't actually do what it says it's supposed to.



Use the Equifax breach or any other newsworthy hack as part of your strategy. Imagine those are your customer records. Walk through the steps of what needs to be done, in what order, by whom, and when. This will make a great playbook to save in the event that something of that magnitude actually does happen by taking a lot of the guess work and panic out of the live situation. Running through the exercise, and deviations of the exercise, not only provide the teams with practice just in case, but also brings up concerns or limitations that may be able to be remediated prior to a real incident. Scatter smaller drills and team specific workshops throughout the year, and perform at least one large incident involving the entire company and an offensive team once a year.

What to include in the tabletop:

- A handout to participants with the scenario and room for notes.
- Current runbook of how security situations are handled.
- Any policy and procedure manuals.
- List of tools and external services.

Post-exercise actions and questions:

- What went well?
- What could have gone better?
- Are any services or processes missing that would have improved resolution time or accuracy?
- Are any steps unneeded or irrelevant?
- Identify and document issues for corrective action.
- Change the plan appropriately for next time.

Tabletop exercises are composed of several key groups or members.

- During a tabletop exercise there should be a moderator or facilitator that will deliver the scenario to be played out. This moderator can answer “what if ” questions about the imaginary emergency as well as lead discussion, pull in additional resources, and control the pace of the exercise. Inform the participants that it is perfectly acceptable to not have answers to questions during this exercise. The entire purpose of tabletops is to find the weaknesses in current processes to mitigate them prior to an actual incident.
- A member of the exercise should also evaluate the overall performance of the exercise as well as create an after-action report. This evaluator should take meticulous notes as well as follow along any runbook to ensure accuracy. While the evaluator will be the main notetaker, other groups and individuals may have specific knowledge and understanding of situations. In this case having each member provide the evaluator with their own notes at the conclusion of the tabletop is a good step.
- Participants make up the majority of this exercise. Included should be groups such as Finance, HR, Legal, Security (both physical and information), Management, Marketing, and any other key group that may be required. Participants should be willing to engage in the conversation, challenge themselves and others politely, and work within the parameters of the exercise.

Me

- ❖ Amanda Berlin
- ❖ @Infosystir
- ❖ Co-Author of “Defensive Security Handbook”
- ❖ Co-host on the Brakeing Down Security podcast
- ❖ Blogger
- ❖ Mom of 3 kick ass boys
- ❖ Lover of unicorns and lock picking



- ❖ <https://www.fireeye.com/blog/threat-research/2016/06/automatically-extracting-obfuscated-strings.html>
- ❖ <http://hackerhurricane.blogspot.com/2016/09/avoiding-ransomware-with-built-in-basic.html>
- ❖ <https://isc.sans.edu/threatfeed.html>
- ❖ <https://www.eventsentry.com/blog/2015/11/trapping-cryptolockercryptowall-with-honey.html>
- ❖ <https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152>
- ❖ <http://www.freeforensics.org/2016/03/proactively-reacting-to-ransomware.html>
- ❖ <https://blogs.technet.microsoft.com/secguide/2014/09/02/blocking-remote-use-of-local-accounts/>
- ❖ https://attack.mitre.org/wiki/Main_Page