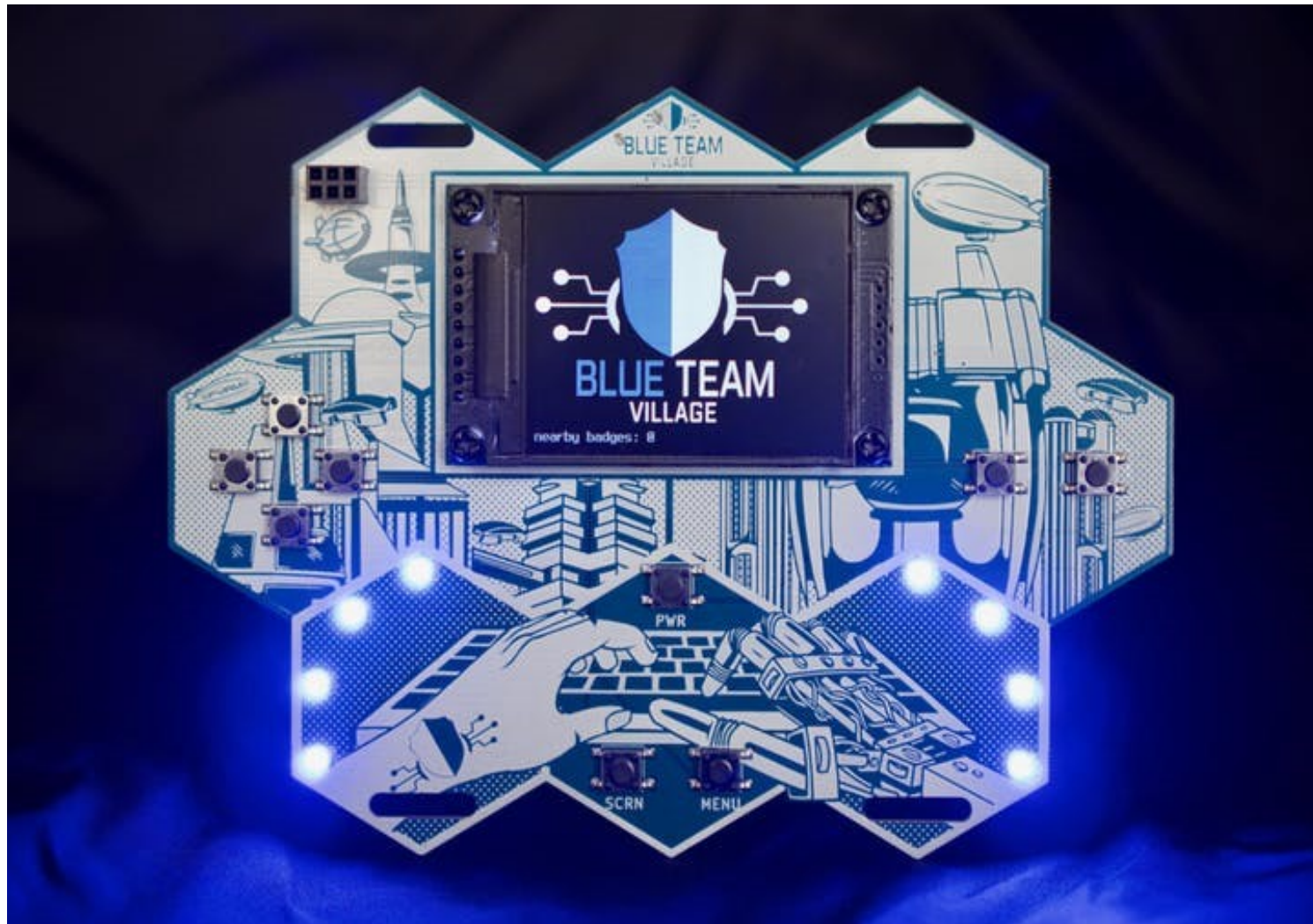


# BTV Capstone Forensic Triage



# **Who Are We**

- **Blue Team Village Capstone/Forensics Team**
- **Blue Team Village Staff**
- **@OMENScan or OMENScan@Gmail.com**
- **FOSS Creator**
  - **OMENS, OMENSApp**
  - **AChoir, AChoirX, AChReport**
- **I Do DFIR Stuff**

# **Disclaimer**

## **ALL OPINIONS ARE MINE ALONE!**

**I do not speak for any past, present, or future employers or their employees, customers or clients. This talk is not endorsed, approved, or otherwise sanctioned by anybody I work for now, or have ever worked for. Ever!**

**In fact, these opinions are mine and mine alone. They might be wrong, and I reserve the right to change my mind at any time without prior notice.**

# **What Is BTV Capstone**

- **Create a Cohesive Integrated Education Program for the Community**
- **Simulate Common Attacks and Attackers**
- **Respond Using Standard Tools and Processes**
  - **Malware Reversing**
  - **Cyber Threat Intel**
  - **Threat Hunting**
  - **DFIR**
- **Build Integrated Training to Share Knowledge**

# **BTV Capstone Forensics**

- **Use Best Practices to Collect Telemetry and Artifacts from the “Compromised” Machines**
- **Use Accepted Forensic Tools to Analyze the Data**
- **Prefer FOSS Tools to Allow Everyone to Play**
- **Describe the Purpose of Each Artifact to Foster Understanding of What They Tell Us, and WHY**
- **Provide the Raw Artifacts for Each Learner to Explore the Data Using Other Tools**

# **BTV Capstone Forensic Triage**

- **General Artifact Collection (Triage) Using AChoir**
- **General Artifact Review Using AChReport**
- **Not Meant to Be Comprehensive**
- **Answer Some Simple Questions:**
  - **Did Something Happen?**
  - **If So, When Did it Happen?**
  - **What Artifacts Can Help Us?**
  - **What Forensic Tools Can Help Us?**
  - **What Should We Look at Next?**



# **BTV Capstone Forensic Triage**

- **Triage Data: Telemetry and Artifacts**
  - **Alpha: EC2AMAZ-C831NP5**
  - **Beta: EC2AMAZ-37OM3IA**
    - **<http://media-origin.blueteamvillage.org/Workshops/ForensicsTable/>**
- **AChoir Collection**
  - **HTML Overview (Alpha & Beta Servers)**
  - **You can use ANY Triage Collection**
- **AchReport**
  - **AchReport Overview (Alpha & Beta Servers)**
  - **You can use ANY Forensic Artifact Parsing Tools!**

# **Identified Indicators from Analysis**

- **Threat Group 1: DRDOOM**
  - **drdoom.notarealfinancialgroup.com**
  - **drdoom.exe**
  - **doom.chm & doom.hta**
- **Threat Group 2: Acid Burn**
  - **acidburn.notarealfinancialgroup.com**
  - **FinDoc.xlsm**
- **Threat Group 3: Fuzzy Poodle**
  - **fuzzypoodle.notarealfinancialgroup.com**
  - **fuzz.exe**



# Actor: DRDOOM

**Name:** EC2AMAZ-C831NP5 (Alpha)

**Artifact:** Browser History

**Tool:** Nirsoft BrowsingHistoryView

**Date:** 7/20/2021 12:50:54 AM

**Telemetry:** Evidence of Download

<http://drdoom.notarealfinancialgroup.com/drdoom.exe>

<http://drdoom.notarealfinancialgroup.com/doom.chm>

<http://drdoom.notarealfinancialgroup.com/doom.hta>

## **What This Tells Us:**

A person logged in as Administrator on this machine browsed to a malicious (Phishing) URL and downloaded drdoom.exe, doom.chm, and doom.hta which are known Remote Access Malware.

	A	B	C	D	E
1	URL	Visit Time	Visit Type	Web Browser	User Profile
2	<a href="http://drdoom.notarealfinancialgroup.com/doom.chm">http://drdoom.notarealfinancialgroup.com/doom.chm</a>	7/20/2021 12:51:49 AM	Download	Firefox	Administrator
3	<a href="http://drdoom.notarealfinancialgroup.com/doom.hta">http://drdoom.notarealfinancialgroup.com/doom.hta</a>	7/20/2021 12:57:34 AM	Download	Firefox	Administrator
4	<a href="http://drdoom.notarealfinancialgroup.com/drdoom.exe">http://drdoom.notarealfinancialgroup.com/drdoom.exe</a>	7/20/2021 12:50:54 AM	Download	Firefox	Administrator
5					

# Actor: DRDOOM

Below is an Index of the Artifacts gathered for Acquisition: ACQ-IR-EC2AMAZ-C831NP5-20210726-1823

B

<<

[Root](#)

[MemDump](#)



[Prf](#)

[RawData](#)

[Reg](#)

## a\ Index of C:\Users\4n6\Desktop\BTV\BTV-DC29\Capstone\Alpha\

 [\[parent directory\]](#)

Name	Size	Date Modified
 <a href="#">BrowseHist.csv</a>	18.5 kB	7/26/21, 11:30:53 AM
 <a href="#">BrowseHist.htm</a>	101 kB	7/26/21, 11:30:53 AM

# Actor: DRDOOM

**Name:** EC2AMAZ-C831NP5 (Alpha)

**Artifact:** HKCU UserAssist Registry Keys

**Tool:** Nirsoft UserAssistView

**Date:** 7/20/2021 12:53:25 AM

**Telemetry:** Evidence of Execution

{F38BF404-1D43-42F2-9305-67DE0B28FC23}\hh.exe

{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\mshta.exe

## **What This Tells Us:**

Time Proximity suggests that the logged in user attempted to open the doom.chm malware (which would run hh.exe) and the doom.hta malware (which would run mshta.exe)

	A	B	C
1	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\mshta.exe	7/20/2021 12:58:03 AM	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2	{F38BF404-1D43-42F2-9305-67DE0B28FC23}\hh.exe	7/20/2021 12:53:25 AM	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
3			
4			

# Actor: DRDOOM

[Root](#)[MemDump](#)[Prf](#)[RawData](#)[Reg](#)

## Index of C:\Users\4n6\Desktop\BTV\BTV-DC29\Capstone\Alpha\

[parent directory]

Name	Size	Date Modified
Nativ/		7/26/21, 11:28:28 AM
Sys32/		7/26/21, 11:28:28 AM
ArpInfo.dat	494 B	7/26/21, 11:29:44 AM
CPorts.csv	16.4 kB	7/26/21, 11:29:44 AM
EnVar.dat	1.6 kB	7/26/21, 11:28:28 AM
IPCfgDNS.dat	73 B	7/26/21, 11:29:44 AM
IPConfig.dat	2.1 kB	7/26/21, 11:29:44 AM
LastActivity.csv	45.9 kB	7/26/21, 11:29:47 AM
Logon.dat	132 B	7/26/21, 11:29:46 AM
NetBios.dat	357 B	7/26/21, 11:29:44 AM
OpenFiles.dat	131 kB	7/26/21, 11:29:44 AM
PSList.dat	84.6 kB	7/26/21, 11:29:42 AM
QFEList.dat	12.6 kB	7/26/21, 11:28:32 AM
SchedTasks.dat	275 kB	7/26/21, 11:29:46 AM
Services-2.dat	66.7 kB	7/26/21, 11:29:46 AM
Services-3.dat	5.9 kB	7/26/21, 11:29:46 AM
Services.dat	2.0 kB	7/26/21, 11:29:46 AM
TaskAll.dat	96.9 kB	7/26/21, 11:29:41 AM
Tasklist.dat	15.3 kB	7/26/21, 11:28:32 AM
UserAssist.csv	8.2 kB	7/26/21, 11:29:47 AM



# Actor: DRDOOM

**Name:** EC2AMAZ-C831NP5 (Alpha)

**Artifact:** Browser History

**Tool:** Nirsoft BrowsingHistoryView

**Date:** 7/20/2021 1:49:30 AM

**Telemetry:** Evidence of Download

<http://drdoom.notarealfinancialgroup.com/cmd.war>

## **What This Tells Us:**

The Actor has downloaded a WebShell (that will then be moved to the Beta server to allow full control of that server).

	A	B	C	D	E	F
1	URL	Title	Visit Time	Visit Type	Web Browser	User Profile
2	<a href="http://drdoom.notarealfinancialgroup.com/cmd.war">http://drdoom.notarealfinancialgroup.com/cmd.war</a>	<a href="#">cmd.war</a>	7/20/2021 1:49:30 AM	Download	Firefox	Administrator
3	<a href="http://drdoom.notarealfinancialgroup.com/cmd.war">http://drdoom.notarealfinancialgroup.com/cmd.war</a>	<a href="#">cmd.war</a>	7/20/2021 1:49:30 AM	Download	Firefox	Default
4						
5						



# Actor: DRDOOM

**Name:** EC2AMAZ-C831NP5 (Alpha)

**Artifact:** Browser History

**Tool:** Nirsoft BrowsingHistoryView

**Date:** 7/20/2021 1:51:35 AM

**Telemetry:** Evidence of Remote Access

<http://172.16.44.102:8080/cmd/cmd.jsp?c=whoami>

## **What This Tells Us:**

The Actor has moved laterally, and compromised 172.16.44.102 (Beta) by installing a WebShell, and is issuing commands to that server.

	A	B	C	D	E
1	URL	Visit Time	Visit Type	Web Browser	User Profile
2	<a href="http://172.16.44.102:8080/cmd.jsp">http://172.16.44.102:8080/cmd.jsp</a>	7/20/2021 1:51:48 AM	Link	Firefox	Administrator
3	<a href="http://172.16.44.102:8080/cmd/?cmd=whoami">http://172.16.44.102:8080/cmd/?cmd=whoami</a>	7/20/2021 1:51:35 AM	Temporary Redirect	Firefox	Administrator
4	<a href="http://172.16.44.102:8080/cmd/cmd.jsp?c=whoami">http://172.16.44.102:8080/cmd/cmd.jsp?c=whoami</a>	7/20/2021 1:54:25 AM	Typed URL	Firefox	Default
5	<a href="http://172.16.44.102:8080/manager/html">http://172.16.44.102:8080/manager/html</a>	7/20/2021 1:50:48 AM	Link	Firefox	Default
6					



# Actor: DRDOOM

**Name:** EC2AMAZ-37OM3IA(Beta)

**Artifact:** HKCU UserAssist Registry Keys

**Tool:** Nirsoft UserAssistView

**Date:** 7/20/2021 2:05:06 AM

**Telemetry:** Evidence of Execution

C:\Users\nssm.exe

## **What This Tells Us:**

The logged in user (HKCU) executed the nssm.exe malware. This was likely to have been uploaded from Alpha to this server via the WebShell – but that is speculation, and needs to be verified via artifacts.

	A	B	C
1	C:\Users\nssm.exe	7/20/2021 2:05:06 AM	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2			
3			
4			
5			
6			

# Actor: DRDOOM

**Name:** EC2AMAZ-37OM3IA(Beta)

**Artifact:** Browser History

**Tool:** Nirsoft BrowsingHistoryView

**Date:** 7/20/2021 12:04:50 AM

**Telemetry:** Evidence of File Access

file:///C:/Users/Administrator/Documents/Customer-Export.zip

## **What This Tells Us:**

The Administrator has accessed an unusually named file (Customer-Export.zip). Further investigation should be done to see what is in this file.

	A	B	C	D
1	URL	Visit Time	Web Browser	User Profile
2	file:///C:/Users/Administrator/Documents/Customer-Export.zip	7/20/2021 12:04:50 AM	Internet Explorer 10/11 / Edge	Default
3	file:///C:/Users/Administrator/Documents/Customer-Export.zip	7/20/2021 12:04:50 AM	Internet Explorer 10/11 / Edge	Administrator
4				
5				
6				

## **DRDOOM: Further Questions**

- **Why Were Doom.CHM and Doom.HTA executed?**
- **How did WebShell: CMD.WAR Get From Alpha to Beta?**
- **What Might Have Been Loaded in Memory?**
- **What Data is in File: Customer-Export.zip**
- **Can We Show if There Was Any Exfil?**
- **What Else Can We Find?**

# Actor: Acid Burn

**Name:** EC2AMAZ-C831NP5 (Alpha)

**Artifact:** Browser History

**Tool:** Nirsoft BrowsingHistoryView

**Date:** 7/20/2021 10:55:14 PM

**Telemetry:** Evidence of Download & Execution

<http://acidburn.notarealfinancialgroup.com/FinDoc.xlsm>

<file:///C:/Users/Administrator/Downloads/FinDoc.xlsm>

## **What This Tells Us:**

A person logged in as Administrator has browsed to, and downloaded a (Phishing) MalDoc and has opened it (likely running the embedded macro malware).

	A	B	C	D	E	F
1	URL	Title	Visit Time	Visit Type	Web Browser	User Profile
2	<a href="http://acidburn.notarealfinancialgroup.com/FinDoc.xlsm">http://acidburn.notarealfinancialgroup.com/FinDoc.xlsm</a>	<a href="#">FinDoc.xlsm</a>	7/20/2021 10:55:14 PM	Download	Firefox	Default
3	<a href="http://acidburn.notarealfinancialgroup.com/FinDoc.xlsm">http://acidburn.notarealfinancialgroup.com/FinDoc.xlsm</a>	<a href="#">FinDoc.xlsm</a>	7/20/2021 10:55:14 PM	Download	Firefox	Administrator
4	<a href="file:///C:/Users/Administrator/Downloads/FinDoc.xlsm">file:///C:/Users/Administrator/Downloads/FinDoc.xlsm</a>		7/20/2021 11:40:31 PM		Internet Explorer 10/11 / Edge	Default
5	<a href="file:///C:/Users/Administrator/Downloads/FinDoc.xlsm">file:///C:/Users/Administrator/Downloads/FinDoc.xlsm</a>		7/20/2021 11:40:31 PM		Internet Explorer 10/11 / Edge	Administrator
6						

# Actor: Acid Burn

**Name:** EC2AMAZ-37OM3IA(Beta)

**Artifact:** System Event Log

**Tool:** MS Event Viewer / MS LogParser

**Date:** 2021-07-20 14:56:47

**Telemetry:** Evidence of Remote Execution  
Event 7045, Service Control Manager

## **What This Tells Us:**

An Actor likely used PSEXec to remotely execute malware on this machine.  
Further investigation needs to be done to identify the specific malware.

	A	B	C	D	
1	Date	ServiceName	ServicePath	ServiceUser	
2	2021-06-29 13:57:48	PSEXESVC	%SystemRoot%\PSEXESVC.exe	LocalSystem	
3	2021-07-20 14:56:47	PSEXESVC	%SystemRoot%\PSEXESVC.exe	LocalSystem	
4	2021-07-20 14:58:03	PSEXESVC	%SystemRoot%\PSEXESVC.exe	LocalSystem	
5	2021-07-20 14:58:37	PSEXESVC	%SystemRoot%\PSEXESVC.exe	LocalSystem	
6	2021-07-20 16:52:13	PSEXESVC	%SystemRoot%\PSEXESVC.exe	LocalSystem	
7					



# Actor: Acid Burn

Below is an Index of the Artifacts gathered for Acquisition: **ACQ-IR-EC2AMAZ-C831NP5-20210726-1823**

<<	<u>Root</u>	<u>MemDump</u>	<u>Prf</u>	<u>RawData</u>	<u>Reg</u>	<u>Evt</u>	<u>SYS</u>
<input type="checkbox"/>	Microsoft-Windows-VPN%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Wcmsvc%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-WFP%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Win32k%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Windows Defender%4Operational.evtx			1.0 MB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Windows Defender%4WHC.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx			1.0 MB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-WindowsSystemAssessmentTool%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-WindowsUpdateClient%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-WinINet-Config%4ProxyConfigChanged.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Winlogon%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-WinRM%4Operational.evtx			1.0 MB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Winsock-WS2HELP%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Wired-AutoConfig%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-WMI-Activity%4Operational.evtx			1.0 MB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-Workplace Join%4Admin.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-WPD-ClassInstaller%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-WPD-CompositeClassDriver%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Microsoft-Windows-WPD-MTPClassDriver%4Operational.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	OAlerts.evtx			68.0 kB		7/1/21, 5:09:17 PM	
<input type="checkbox"/>	Security.evtx			3.1 MB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Setup.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	SMSApi.evtx			68.0 kB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	System.evtx			2.1 MB		6/8/21, 11:11:57 PM	
<input type="checkbox"/>	Windows PowerShell.evtx			11.1 MB		6/8/21, 11:11:57 PM	



# Actor: Acid Burn

LogParser.exe "Select TimeGenerated AS Date,  
EXTRACT\_TOKEN(strings, 0, '|') AS ServiceName,  
EXTRACT\_TOKEN(strings, 1, '|') AS ServicePath,  
EXTRACT\_TOKEN(strings, 4, '|') AS ServiceUser  
FROM System.evtx WHERE EventID = 7045"

	A	B	C	D
1	Date	<u>ServiceName</u>	<u>ServicePath</u>	<u>ServiceUser</u>
2	2021-06-15 19:05:52	MpKsld6af4f2b	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{907F2FBB-598C-438E-81B3-61C0705FA412}\MpKsldrv.sys	
3	2021-06-15 19:47:24	Sysmon64	C:\Windows\Sysmon64.exe	<u>LocalSystem</u>
4	2021-06-15 19:47:24	<u>SysmonDrv</u>	C:\Windows\SysmonDrv.sys	
5	2021-06-15 19:47:47	<u>winlogbeat</u>	C:\Program Files\winlogbeat\winlogbeat.exe -environment=windows_service -c "C:\Program Files\winlogbeat\winlogbeat.yml" -path.home "C:\Program Files\winlogbeat" -path.data "C:\ProgramData\winlogbeat" -path.logs "C:\ProgramData\winlogbeat\logs" -E logging.files.redirect_stderr=true	<u>LocalSystem</u>
6	2021-06-27 12:43:35	MpKslead2980e	C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{DB11B8EC-FC22-4E84-9C48-1C0F94A44273}\MpKsldrv.sys	
7	2021-06-29 13:57:48	PSEXESVC	%SystemRoot%\PSEXESVC.exe	<u>LocalSystem</u>
8	2021-07-20 14:56:47	PSEXESVC	%SystemRoot%\PSEXESVC.exe	<u>LocalSystem</u>
9	2021-07-20 14:58:03	PSEXESVC	%SystemRoot%\PSEXESVC.exe	<u>LocalSystem</u>
10	2021-07-20 14:58:37	PSEXESVC	%SystemRoot%\PSEXESVC.exe	<u>LocalSystem</u>
11	2021-07-20 16:52:13	PSEXESVC	%SystemRoot%\PSEXESVC.exe	<u>LocalSystem</u>
12	2021-07-26 12:11:03	<u>pmem</u>	C:\Users\ADMINI~1\AppData\Local\Temp\pme9C0B.tmp	
13				

## **Acid Burn: Further Questions**

- **Can We Get the FinDoc.xlsm MalDoc?**
- **What Malware did FinDoc.xlsm Drop?**
- **What malware did PSExec Run on Beta?**
- **What Might Have Been Loaded in Memory?**
- **Can We Show if There Was Any Exfil?**
- **What Else Can We Find?**

# Actor: Fuzzy Poodle

**Name:** EC2AMAZ-C831NP5 (Alpha)

**Artifact:** Browser History

**Tool:** Nirsoft BrowsingHistoryView

**Date:** 7/19/2021 11:23:38 PM

**Telemetry:** Evidence of Download

<http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz.exe>

<http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz1.exe>

## What This Tells Us:

A person logged in as Administrator on this machine browsed to a malicious (Phishing) URL and downloaded fuzz.exe and, fuzz1.exe which are known Remote Access Malware.

	A	B	C	D	E
1	URL	Visit Time	Visit Type	Web Browser	User Profile
2	<a href="http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz.exe">http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz.exe</a>	7/19/2021 11:23:38 PM	Download	Firefox	Default
3	<a href="http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz.exe">http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz.exe</a>	7/19/2021 11:23:38 PM	Download	Firefox	Administrator
4	<a href="http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz1.exe">http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz1.exe</a>	7/19/2021 11:27:31 PM	Download	Firefox	Administrator
5	<a href="http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz1.exe">http://fuzzypoodle.notarealfinancialgroup.com:8081/fuzz1.exe</a>	7/19/2021 11:27:31 PM	Download	Firefox	Default
6					

# Actor: Fuzzy Poodle

**Name:** EC2AMAZ-C831NP5 (Alpha)

**Artifact:** HKCU UserAssist Registry Keys

**Tool:** Nirsoft UserAssistView

**Date:** 7/19/2021 11:25:15

**Telemetry:** Evidence of Execution

C:\Users\Administrator\Downloads\fuzz.exe

C:\Users\Administrator\Downloads\fuzz1.exe

## **What This Tells Us:**

A person logged in as Administrator on this machine executed the fuzz.exe and fuzz1.exe programs which are known malicious remote access malware.

	A	B	C	D
1	C:\Users\Administrator\Downloads\fuzz.exe	43	17/19/2021 11:25:15 PM	
2	C:\Users\Administrator\Downloads\fuzz1.exe	44	17/19/2021 11:28:44 PM	
3				
4				



# Actor: Fuzzy Poodle

**Name:** EC2AMAZ-C831NP5 (Alpha)

**Artifact:** AmCache.hve

**Tool:** Harlan Carvey's RegRipper

**Date:** 2021-07-19 23:25:17

**Telemetry:** Evidence of Execution

C:\Users\Administrator\Downloads\fuzz.exe

C:\Users\Administrator\Downloads\fuzz1.exe

## **What This Tells Us:**

A person logged in as Administrator on this machine executed the fuzz.exe and fuzz1.exe programs which are known malicious remote access malware.

```
amcache v.20200515  
(amcache) Parse AmCache.hve file
```

```
***InventoryApplicationFile***
```

```
c:\users\administrator\downloads\fuzz.exe  LastWrite: 2021-07-19 23:25:17Z  
Hash: 8ec3371e9a666f1f5383348be27c9662df345cec
```

```
c:\users\administrator\downloads\fuzz1.exe  LastWrite: 2021-07-20 00:13:33Z  
Hash: bac3f1660e0b937ee4e77bfc6ad3334f693ed9a7
```

# Actor: Fuzzy Poodle

**Name:** EC2AMAZ-C831NP5 (Alpha)

**Artifact:** System Event Log

**Tool:** MS Event Viewer / MS LogParser

**Date:** 2021-07-19 16:39:50

**Telemetry:** Evidence of Persistence  
Event 7045, Service Control Manager

## What This Tells Us:

An Actor, logged in as Administrator (RID 500) on this machine executed the nssm.exe program to create a service called FuzzService - Malware persistence for fuzz1.exe

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: FuzzService  
Service File Name: C:\Users\Administrator\Downloads\nssm.exe  
Service Type: user mode service  
Service Start Type: auto start  
Service Account: LocalSystem

Log Name: System  
Source: Service Control Manager  
Event ID: 7045  
Level: Information  
User: S-1-5-21-1976052002-3724303175-1599532400-500  
OpCode: Info  
More Information: [Event Log Online Help](#)

Logged: 7/19/2021 4:39:50 PM  
Task Category: None  
Keywords: Classic  
Computer: EC2AMAZ-C831NP5.avengers.local

S-1-5-21-1976052002-3724303175-1599532400-500



# **Fuzzy Poodle: Further Questions**

- **Why Did the Actor Execute both Fuzz.EXE and Fuzz1.EXE?**
- **What Might Have Been Loaded in Memory?**
- **Is There Evidence of Lateral Movement ?**
- **Can We Show if There Was Any Exfil?**
- **What Else Can We Find?**

## **BTV Capstone: Further Questions**

- **3 Actors Are in the Environment. How Do We Separate Their Activity? Are They Related?**
- **Is There a Likely Compromise? If So, When Did it Likely Start?**
- **What Should We Look at/for Next?**
- **What Should We Do Next?**
- **Can We Show if There Was Any Exfil?**
- **What Else Can We Find?**

# Questions ?

**Thanks For Hanging Out !**

**Now. Go download the Telemetry and Artifacts yourself - and let us know what you find! Use whatever tools you like!**

**Twitter:** @OMENScan, @BlueTeamVillage

**Email:** [OMENScan@GMail.com](mailto:OMENScan@GMail.com)

**Web:** [www: MuSecTech.com](http://www.MuSecTech.com), [www.blueteamvillage.org](http://www.blueteamvillage.org)

**Discord:** [discord.com/invite/blueteamvillage](https://discord.com/invite/blueteamvillage)