Project Obsidian

Forensics: Kill Chain 3

Continued Adventures in Splunk and Security Onion

ExtremePaperClip & Wes Lambert

Who are these guys, again?

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 3: Agenda

- Data Sources
- RDP
- Recon
- Portscan
- Kerberoasting
- Dumping Processes
- Dumping SAM database
- Adding Users
- Wiping Event Logs
- Summary of Findings

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

The Adventure Continues

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/

Remind me…
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)

RDP

SPLUNK: ENDPOINT LOGS

March 7, 2022

We (still) need to talk about RDP

Brett Winterford

Quarter by quarter, for three years now, abuse of Remote Desktop Protocol (RDP) has been the most common root cause of all ransomware events.

It's no surprise why RDP makes for an attractive target: RDP is the primary vehicle for remote access to Windows servers and is used for administrative functions. It's the most commonly listed method of remote access sold by initial access brokers.

According to some 2019 research [pdf] by Sophos, an open RDP port gets its first connection request somewhere between 90 seconds and 15 hours of being exposed on the internet. Brute forcing RDP is so easy, the researchers noted, that "the criminal gangs who conduct targeted ransomware attacks have almost entirely abandoned alternative methods of network entry."

> "In recent years, criminals deploying targeted ransomware like BitPaymer, Ryuk, Matrix, and SamSam have almost completely abandoned other methods of network ingress in favor of using RDP. Gangs like these have the choice of cracking passwords themselves using tools like NLBrute, buying passwords cracked by others, or buying accounts on compromised RDP servers."

The situation hasn't improved much since then. According to a joint statement released by authorities in the US, UK and Australia in February, ransomware actors assumed that organizations rushing to provide remote access during the first COVID lockdowns would misconfigure RDP. And oh boy, were they right.

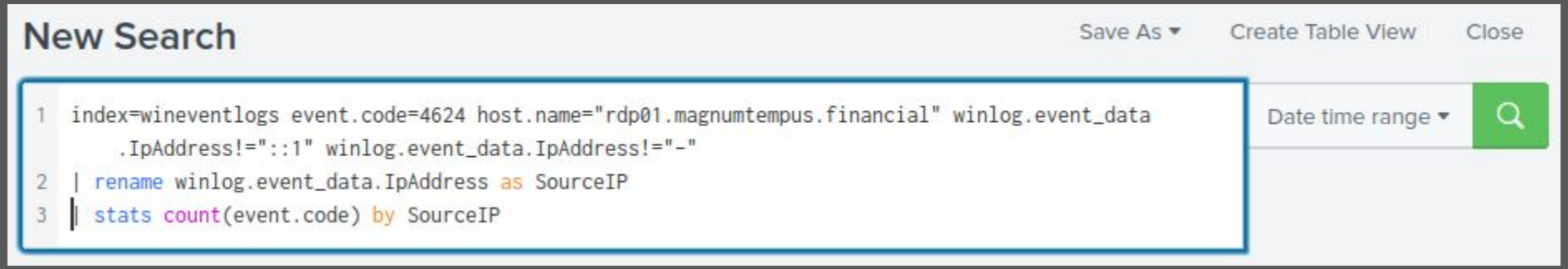
Source: https://sec.okta.com/weneedtotalkaboutrdp

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:00 *to* 02/19/22 23:59

Splunk Search:

```
index=wineventlogs event.code=4624
host.name="rdp01.magnumtempus.financial"
winlog.event data.IpAddress!="::1" winlog.event data.IpAddress!="-"
| rename winlog.event data.IpAddress as SourceIP
| stats count(event.code) by SourceIP
```



SPLUNK: ENDPOINT LOGS

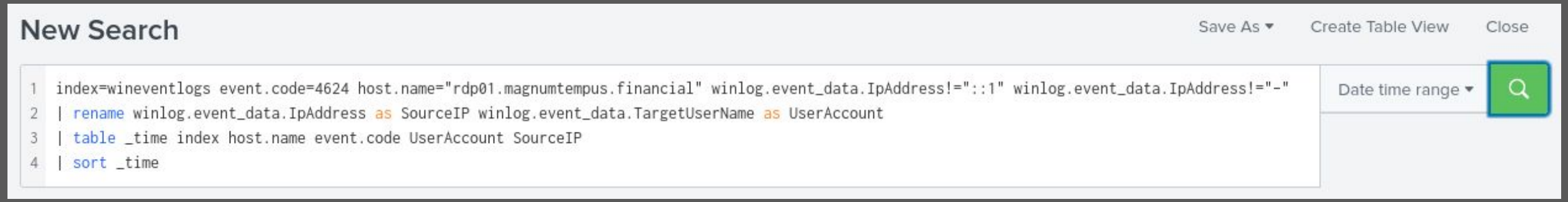
SourceIP	count(event.code)
172.16.21.100	2
172.16.50.110	4
3.129.164.140	8

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:00 *to* 02/19/22 23:59

Splunk Search:

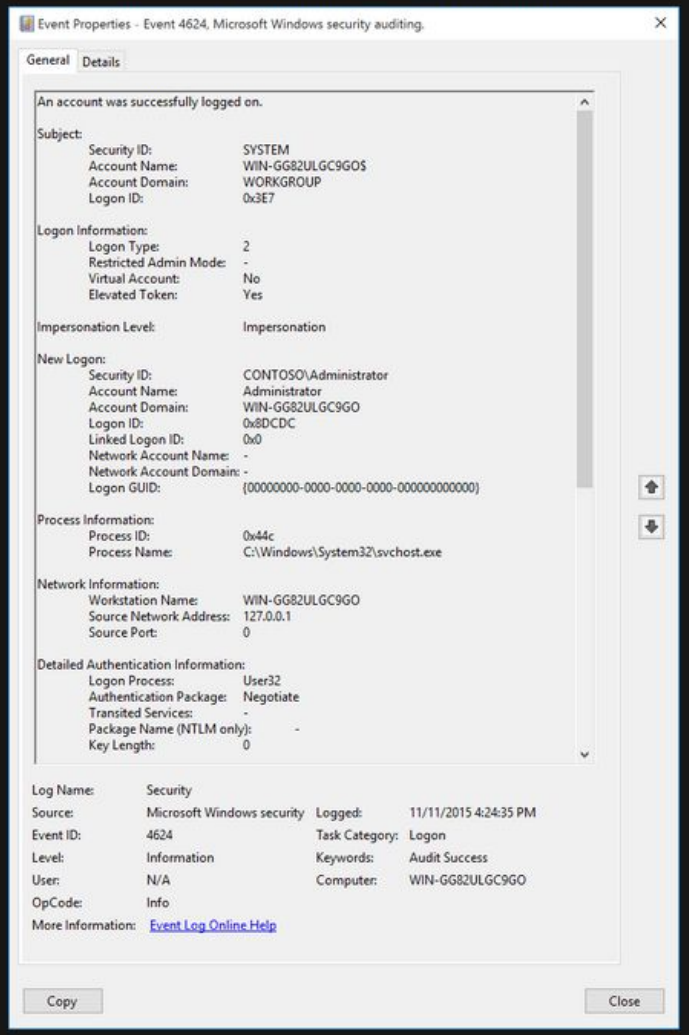
```
index=wineventlogs event.code=4624
host.name="rdp01.magnumtempus.financial"
winlog.event data.IpAddress!="::1" winlog.event_data.IpAddress!="-" |
rename winlog.event data.IpAddress as SourceIP
winlog.event data.TargetUserName as UserAccount | table _time index
host.name event.code UserAccount SourceIP | sort _time
```



SPLUNK: ENDPOINT LOGS

4624(S): An account was successfully logged on.

Article • 12/14/2021 • 14 minutes to read • 13 contributors



Source: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	UserAccount	SourceIP
2022-02-19 20:08:32.358	wineventlogs	rdp01.magnumtempus.financial	4624	brent.socium	3.129.164.140
2022-02-19 20:08:32.359	wineventlogs	rdp01.magnumtempus.financial	4624	clarie.insigni	3.129.164.140
2022-02-19 20:08:33.466	wineventlogs	rdp01.magnumtempus.financial	4624	dale.phasle	3.129.164.140
2022-02-19 20:08:36.660	wineventlogs	rdp01.magnumtempus.financial	4624	norma.gene	3.129.164.140
2022-02-19 20:08:36.661	wineventlogs	rdp01.magnumtempus.financial	4624	pat.risus	3.129.164.140
2022-02-19 20:11:18.753	wineventlogs	rdp01.magnumtempus.financial	4624	pat.risus	3.129.164.140
2022-02-19 20:11:20.762	wineventlogs	rdp01.magnumtempus.financial	4624	pat.risus	3.129.164.140
2022-02-19 20:11:20.762	wineventlogs	rdp01.magnumtempus.financial	4624	pat.risus	3.129.164.140
2022-02-19 22:29:14.875	wineventlogs	rdp01.magnumtempus.financial	4624	Administrator	172.16.21.100
2022-02-19 22:29:18.978	wineventlogs	rdp01.magnumtempus.financial	4624	Administrator	172.16.21.100
2022-02-19 22:56:57.148	wineventlogs	rdp01.magnumtempus.financial	4624	Administrator	172.16.50.110
2022-02-19 22:56:57.149	wineventlogs	rdp01.magnumtempus.financial	4624	Administrator	172.16.50.110
2022-02-19 22:56:57.149	wineventlogs	rdp01.magnumtempus.financial	4624	Administrator	172.16.50.110
2022-02-19 22:56:57.149	wineventlogs	rdp01.magnumtempus.financial	4624	Administrator	172.16.50.110

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 20:00 *to* 02/19/22 23:59

	Count	rule.name	event.module	event.severity_label
	301	ET POLICY DNS Update From External net	suricata	high
	127	ET RPC DCERPC SVCCTL - Remote Service Control Manager Access	suricata	high
	12	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)	suricata	high
	12	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	suricata	high
	1	ET MALWARE Interactsh Control Panel (DNS)	suricata	high
	2,112	ET POLICY PsExec service created	suricata	medium
	426	ET POLICY SMB2 NT Create AndX Request For an Executable File	suricata	medium
	333	ET POLICY SMB Executable File Transfer	suricata	medium
	46	ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement	suricata	medium
	21	ET INFO Observed DNS Query to .cloud TLD	suricata	medium
	15	ET DNS Query for .to TLD	suricata	medium
	8	ET INFO Interactsh Domain in DNS Lookup (.interact .sh)	suricata	medium
	6	ET INFO Interactsh Domain in DNS Lookup (.interactsh .com)	suricata	medium
	2	ET POLICY Observed DNS Query to File Transfer Service Domain (transfer .sh)	suricata	medium
	220	ET POLICY RDP connection confirm	suricata	low
	36	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	suricata	low
	6	ET POLICY MS Remote Desktop Administrator Login Request	suricata	low
	3	ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in TLS SNI)	suricata	low
	2	ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in DNS Lookup)	suricata	low
	2	ET INFO Windows OS Submitting USB Metadata to Microsoft	suricata	low
	1	ET INFO Windows Powershell User-Agent Usage	suricata	low
	1	ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection	suricata	low
	1	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)	suricata	low

SECURITY ONION: NETWORK LOGS

SECURITY ONION: NETWORK LOGS

Timestamp ▲	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port
2022-02-19 20:08:30.475 +00:00	ET POLICY RDP connection confirm	low	172.16.55.110	3389	3.129.164.140	35958
2022-02-19 20:08:30.486 +00:00	ET POLICY RDP connection confirm	low	172.16.55.110	3389	3.129.164.140	35960
2022-02-19 20:08:30.508 +00:00	ET POLICY RDP connection confirm	low	172.16.55.110	3389	3.129.164.140	35962
2022-02-19 20:08:30.516 +00:00	ET POLICY RDP connection confirm	low	172.16.55.110	3389	3.129.164.140	35964
2022-02-19 20:08:30.884 +00:00	ET POLICY RDP connection confirm	low	172.16.55.110	3389	3.129.164.140	35958
2022-02-19 20:08:30.891 +00:00	ET POLICY RDP connection confirm	low	172.16.55.110	3389	3.129.164.140	35960
2022-02-19 20:08:30.899 +00:00	ET POLICY RDP connection confirm	low	172.16.55.110	3389	3.129.164.140	35966

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

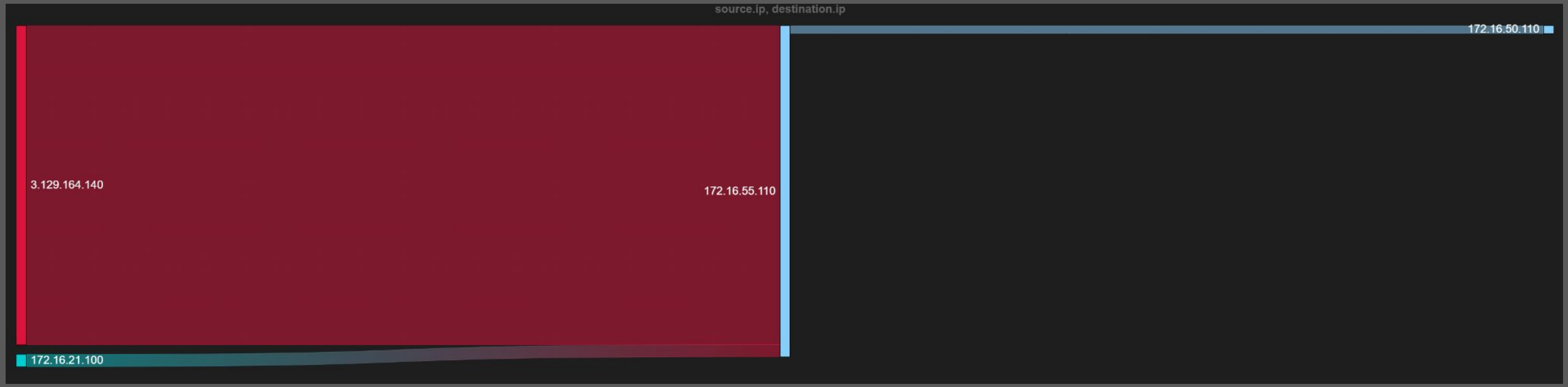
```
"172.16.55.110" AND event.dataset:rdp | groupby source.ip
destination.ip
```

SECURITY ONION: NETWORK LOGS

Count	source.ip	destination.ip
211	3.129.164.140	172.16.55.110
8	172.16.21.100	172.16.55.110
5	172.16.55.110	172.16.50.110

SECURITY ONION: NETWORK LOGS

```
"172.16.55.110" AND event.dataset:rdp | groupby -sankey source.ip destination.ip
```



SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
destination.ip:"172.16.55.110" AND event.dataset:rdp | groupby source.ip destination.ip
```

SECURITY ONION: NETWORK LOGS

Count	source.ip	destination.ip
211	3.129.164.140	172.16.55.110
8	172.16.21.100	172.16.55.110

SECURITY ONION: NETWORK LOGS

```
destination.ip:"172.16.55.110" AND event.dataset:rdp | groupby -sankey source.ip destination.ip
```

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

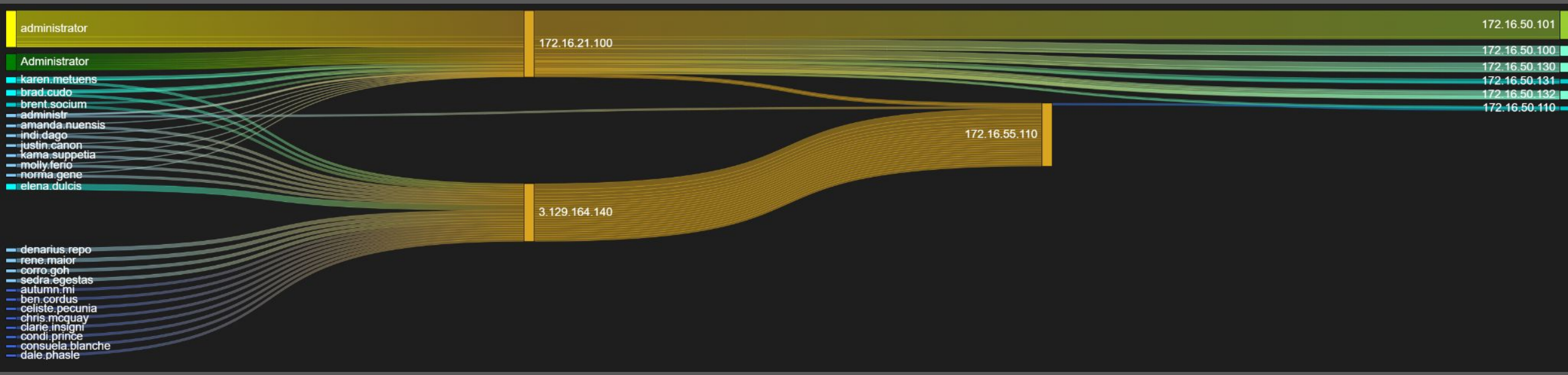
```
event.dataset:rdp | groupby @timestamp rdp.cookie source.ip
destination.ip
```

SECURITY ONION: NETWORK LOGS

2022-02-19T20:08:30.471Z	amanda.nuensis	3.129.164.140	172.16.55.110
2022-02-19T20:08:30.482Z	autumn.mi	3.129.164.140	172.16.55.110
2022-02-19T20:08:30.513Z	autumn.mi	3.129.164.140	172.16.55.110
2022-02-19T20:08:30.521Z	amanda.nuensis	3.129.164.140	172.16.55.110
2022-02-19T20:08:30.895Z	ben.cordus	3.129.164.140	172.16.55.110
2022-02-19T20:08:30.903Z	ben.cordus	3.129.164.140	172.16.55.110
2022-02-19T20:08:30.932Z	brad.cudo	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.079Z	brad.cudo	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.115Z	brent.socium	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.126Z	brent.socium	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.183Z	celiste.pecunia	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.251Z	celiste.pecunia	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.327Z	chris.mcquay	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.363Z	chris.mcquay	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.448Z	clarie.insigni	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.538Z	clarie.insigni	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.577Z	condi.prince	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.737Z	condi.prince	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.785Z	connie.mendax	3.129.164.140	172.16.55.110
2022-02-19T20:08:31.890Z	connie.mendax	3.129.164.140	172.16.55.110
2022-02-19T20:08:32.042Z	consuela.blanche	3.129.164.140	172.16.55.110
2022-02-19T20:08:32.093Z	corro.goh	3.129.164.140	172.16.55.110
2022-02-19T20:08:32.290Z	corro.goh	3.129.164.140	172.16.55.110
2022-02-19T20:08:32.350Z	corro.goh	3.129.164.140	172.16.55.110
2022-02-19T20:08:32.385Z	dale.phasle	3.129.164.140	172.16.55.110

SECURITY ONION: NETWORK LOGS

```
event.dataset:rdp | groupby -sankey rdp.cookie source.ip destination.ip
```



Recon

SPLUNK: ENDPOINT LOGS

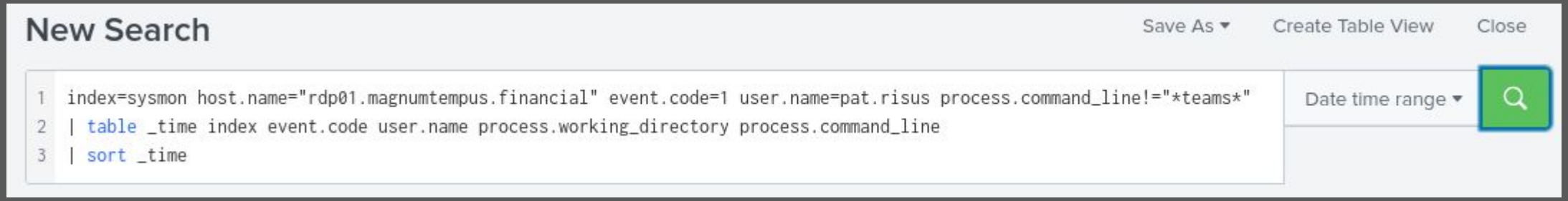
Image Source: https://commons.wikimedia.org/wiki/File:Cyan_gradient_grimacing_face_emoji.svg

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:00 *to* 02/19/22 23:59

Splunk Search:

```
index=sysmon host.name="rdp01.magnumtempus.financial" event.code=1
user.name=pat.risus process.command_line!="*teams*"
| table  time index event.code user.name process.working_directory
process.command_line
| sort  _time
```



SPLUNK: ENDPOINT LOGS

_time	index	event.code	user.name	process.working_directory	process.command_line
2022-02-19 20:11:38	sysmon	1	pat.risus	C:\Windows\system32\	C:\Windows\System32\Rundll32.exe C:\Windows\System32\Migration\WininetPlugin.dll,MigrateCacheForUser /m /0
2022-02-19 20:11:39	sysmon	1	pat.risus	C:\Windows\system32\	"C:\Windows\System32\unregmp2.exe" /FirstLogon
2022-02-19 20:11:40	sysmon	1	pat.risus	C:\Windows\system32\	rundll32.exe AppXDeploymentExtensions.OneCore.dll,ShellRefresh
2022-02-19 20:11:40	sysmon	1	pat.risus	C:\Windows\system32\	"C:\Program Files\Google\Chrome\Application\98.0.4758.102\Installer\chrmstp.exe" --type=crashpad-handler /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Windows\TEMP\Crashp --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=9 --initial-client-data=0x228,0x22c,0x230,0x204,0x234,0x7ff771f4e468,0x7ff771f4e478,0x
2022-02-19 20:11:40	sysmon	1	pat.risus	C:\Windows\system32\	"C:\Program Files\Google\Chrome\Application\98.0.4758.102\Installer\chrmstp.exe" --configure-user-settings --verbose-logging --system- --channel=stable
2022-02-19 20:12:04	sysmon	1	pat.risus	C:\Windows\system32\	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoProfi -NonInteractive -NoLogo -WindowStyle hidden -ExecutionPolicy Unrest "Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psd1"; Set-Wallpaper -Initial"
2022-02-19 20:12:04	sysmon	1	pat.risus	C:\Windows\SysWOW64\	C:\Windows\SysWOW64\runonce.exe /Run6432
2022-02-19 20:12:04	sysmon	1	pat.risus	C:\Windows\system32\	C:\Windows\system32\cmd.exe /c ""C:\Users\pat.risus\AppData\Roaming\Windows\Start Menu\Programs\Startup\RunWallpaperSetupInit.cmd" "
2022-02-19 20:12:16	sysmon	1	pat.risus	C:\Users\pat.risus\	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

SPLUNK: ENDPOINT LOGS

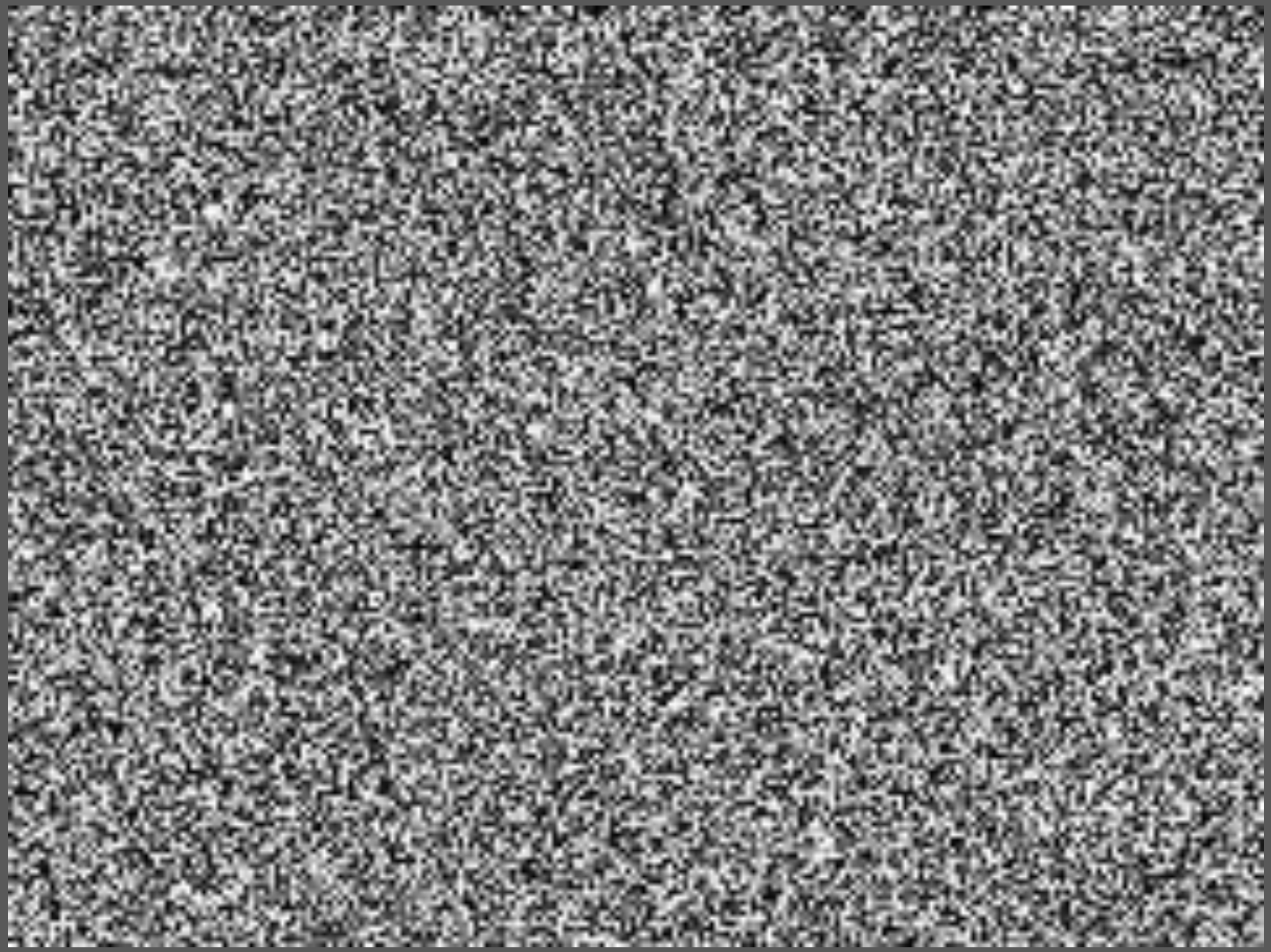


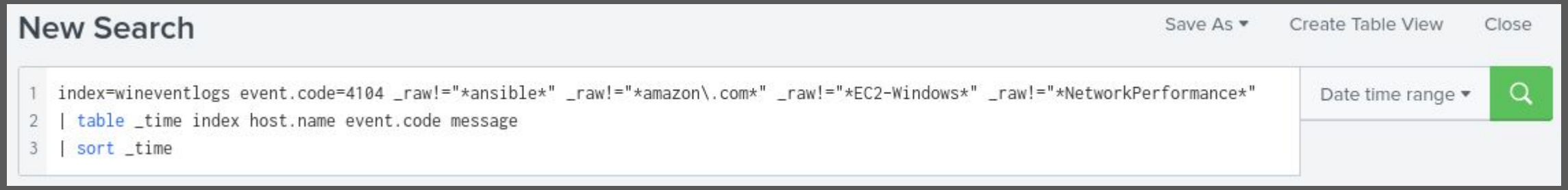
Image Source: https://commons.wikimedia.org/wiki/File:White-noise-mv255-240x180.png

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:12 *to* 02/19/22 23:59

Splunk Search:

```
index=wineventlogs event.code=4104  raw!="*ansible*"
 raw!="*amazon\.com*"  raw!="*EC2-Windows*"
 raw!="*NetworkPerformance*"
| table  time index host.name event.code message
| sort  _time
```



SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	message
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:12 *to* 02/19/22 23:59

Splunk Search:

```
index=wineventlogs event.code=4104  raw!="*ansible*"
 raw!="*amazon\.com*"  raw!="*EC2-Windows*"
 raw!="*NetworkPerformance*"
| table  time index host.name event.code  _raw
| sort  _time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	_raw
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	{"event":{"action":"Execute a Remote Command","kind":"event","code":"4104","created":"2022-02-19T20:12:55.522Z","provider":"Microsoft-Windows-PowerShell"},"agent":{"hostname":"rdp0 {"kernel":"10.0.14393.4770 (rs1_release.211101-1440)","family":"windows","build":"14393.4770","version":"10.0","type":"windows","name":"Windows Server 2016 Datacenter","platform":"w text (15 of 56):\nHuO2iG3Gf+3lMAIZx/buoKcTZUT5GFWjWFmmCsvnMAS3xtkXngvgLSiwsUZ0j0xJ2zV5aF1yTUr2/ULzwDYcfvpN7WMQ1W0jHHgeBUY5cDQFxjhwFDjbxsnP/HrwCO1uotcxiXXTzOram+BvtUGxRORZpNHYGFNU9d5 /bXp2S9g68o3oy0QZBnSn7IeXQrldBR2V54EgCEkiOsRuHnTukl2M33yEsKp7PsE7KPoB1CH2Hlcunkcdej/xMFDF7sIpstg+OBYaESBFyWAxBr+dU6oyBeSNXmZVBHvkjoGVa7G1uvoOe6eeB/xBIhLqUCDKnEhCZOGdG5UyIjId4j+/Nhqa /xhNXj7DMc5nvY7OupGygqahJhFfu6njMTaFkMa9hiIJTcKwmiCBVwU3I6XVWkkzKKoGQclpn9jwdQdiaVrmCqlm1n7Xh3PdZtxUa699haGbYcyt699PQeKjWEHAeBmt6+9GIC21Sydjffui036pCVKIzwEhMYZnHRg7a41gR5P4OMTpwgshX /EBAMueyON0jwN89S0LoXzFAsCJcB7k7HmQ58+DrJkHWTUP0jcXcnATFhBSSjZ5xI3VQIEgQafgPIlRpGuNjGIZcnzDwHbTOgtfKa6Gu1OZsZxrgrZVMA8a+B9cn2DOAdo6Jv0P30Z+IemjDosX0mk6ZiSWq1KnSs61jrkNlxIjSxMydyRvkk /J1IGTKb1O5Dv4AQM1gGadd8NKEZceUHx30b1vFIppyoGdRsx34xi8rf6PPU3H0wqNIdOnSsWGNymEps4g3bG328M2FledSfh8T9ScX2K5VAakdWbe3q6+epc6QkdGhknYhwWUWFPSnqVbTTH0PX+RDKJxXye+mVzLxeySCfJvqa2EqfOqgP /5nkfVQvztAruf8grR3GJG9A2Z1w+8mW8XwI/kI3MDCSilppbi8GQUx4eVnpEhbLW1DuOmPmo3ShmAEMLtjG0aZwzB1lW43h94IBBt/srKc0w3BAkQzG0vnJfUzt3Pk+GNxWphizIafmZd4KaTt57Sq/nt2Vz9iPP6kX+JGnIlNLXELzuIWLN /ZESLsNmcm8afsAJSES6uNPcE0SrUqESwJANMZTpKfRO6Cr7yVpgKQw5aCDoYGUMm/M2cMwgVQvs4JRNuRi2ZlwBZSSGUpjOwbP5IdMl7ogiPoZR6voGr4/uaHYnIQhhMjZwZigI0GEi5umEtx0/5nFJmdfyTnteTkrOa7UoizyY2nYW4cfR2 /0rLHhZ01vPHe9GDDGtg4khP0jFOAOlwZtO0TmLz9ql8aqmMQFRIxhEe4MqIRSQ2qjoHB/nG3cGGDcwszg0DMSXkM8w2NfqXnGolv95FsoCTeHTwcBAcd4DoSEKaOHzGNKKYn+zyoxvbr+yPbZFymvrmz0JwtC7WNgeajt8MPDTEnUb6ZKN8 /LOaE54FbY32gd4LeIz8xncILicvB9A7xXo1Ykz+tuXpNjeKrTzlHwQs1hKIh5Nw9uk26a+w9LCTxF/Ymnh+wVdG3s1Rva2r2TnNTx7XEY5EJWESVjuubwy4rPLSQUIPyjkFxxROZSwj6AcL20wSxuneKEGk6J/djXb0lZoF80IPHAAU /UiiKDd4Hq2NRpH+EOTtYzgdlQWgcZEDfKH2q8At6jwOF7iUTmUay3NR6REeABxXo6BDeZU++XMt1hQqUnlccAbfcCT78v8BDr6dGofkel9WOjqB8mudQmx+9Lm0YY09dwEf7hPtwLNEW+iNFeQiH83zWPNYYcsYiOiCBhdGXfDKbjOypKuMI /h/ylxlNuZU9qZ18emM2qOAHuqsw8jAcde1LBN8HdwqXVJ6Ozm79bIc9u7lv+6C2wYFge7MTykg+CcVf4OSJQdP/teULZpy+hqeLovLRp4gEW/CYHkgi3YNDS93H4+/2cvwIk+RsOhD/T43UH8nG257Kzhqc4FCzVEZZWeFBI4SB56hO0O8wD /gG/kYyDQJAw5EglWRNfyk4A90illsXXgcHiRgCxmF12O7r2S2JsAJCEiQSASrBZ0iab0xQkxt6B8S6ZuGdrecqxbYF35oeHf7wsGRgo7xPzYcbzrzMJi3jcsRVZ9d3q6UYynbslfGIijKL/dWiXqoI9/LZiKaXlULDsMWXMqkwjSfZobDqRW /KXSbuFGBgqcRCNwJgLjRAprfAZ3R+ALkuBsBMYJDht0LdYK4sXBN0AoUMQjZsXy78TQIcrq0b6ecJXa3htoKAXPx1F0HQ8rdMJB3OS6llrn75yppenL4A2dnxm5QUr+1iPIASbyMYLfuAB4wwK2mmtS8juPqK/QueEhhRxepbJNa7jYyJZut /r5YZwasgXC1blWMu17LfZpmvd5He7VhOX7bAStHxnfCVE3TR0+a6UNlmwbenJZNyMazdV2o2NvGtB6ZDUXzT2YZFhA83NKLKxjoLhLyo4lSmVPQs1OViTQzU1cyoiB5PNLGZzc2RTco3zBje4ztTmO2AN6zp+hjEDDSk3hJtPDXxM282OP4Q /hvBkTcbwxq2MJUWI9/Bjpn7rLmqjTmRjTusZoV2emPpUtjdyXyIb4eeMe5UrPz4VrQnzqmNaEJypOZ3Hx5lR0bmNQrbWE8ECRuB0LBvc2dNtvSUVniBZHa7I3s0i5LSVX+5QUVvtM0+fuNd3uYkobVRkv/V+Vsbs4v3tPkXivpHw9nsSiBBS /Oh+U8Cm00RN8uWWRElm9EhCZ30m3sCe+Rc+YoZSkq+LHyR0IxGUdoqLlI2m2L6DFAF8ahMVwXQQfYCT3xPtbq0CEMNPIS2PSgON+OQgce6RLrLxK1nt/0A/6wAXRMW18T4l2QS/GPURXbHU0Qy9jgNiFvN67Fy/Jczx4nbsQDH7doBUu4RMV /XDydvughQ1J3gU1S30EyB9Uvgd7Gz51rYjAGIW6ZltKrLLSLYeH90+mQyEW4Xcm5lRNq69dNqafe40vfZR2VVp7Ld7EgHot3ujfis7Hv6viKyeaqXAa5MBetiy3rL2h5wbNHrU6NiE/9aE/48J/3Fl5b9UoiAQ4SK1PcE0Zbo3sz7aB3kX0v /5djzGPR2uA+nBuG6NPuFjndQshvAr6bZSY67ffI8XC3dN8t3Xukq+LvVeOFPA8ywBtbqXMSzsDQJjshLndBxN0btdXSrpNrVwDfTenfTbznVEbE7H0RgLHhD9bhchMJiBCrQblMC99NHX1YzL4P+2qVYA/n9TgpY8VDs42oVXKyEAoJxpdxU /jSp55n6Fi97mbsbfNVcSdu+Ounpil Zh9L47nglBcxcz+Xu7u9ypm72ADycUnJzmooynsKFImIqTQTw6jZMk0pU8Ijd/wpldA5ZQeBXE+PzWez+9PJefzL5a1xMe9ny7HZp7ROTP4BzGf0cb3q4SenkEp0P6AHLT3q0F7f0LeoM59Jp2rx+ft /byqWoR31N5P8t8M0QaY1fY1EID4laOYgPvJwBFYgi2Ct6B29kWr9vlWtha9M2Y2Vb0nxWuLT6Skgo0ePss9kW2N1WIb6ceYtz+uEqKHlmYM4zOUBC2jXWW90jPW7iYrg/XhYqM7tX2BUuSpzO6UMVxsdgtv9ONU7r1q/5hx1hvDOcKZT5GPo /QyLN15oIJblUSid54sBku1EqfSIV2SSuVn3KLJLmSDQHo9utVzyOkbnTsikwDQIz52xvbClXTFXYTd3g+c2wcZR0S6KY6WZiEYcFWU1qvmzfiGyfFX/nhMcGmkmIgpS6fI68MkfTClGb39qT89T2aH30GWSdkZeJ2Qeokk/h9CT6cK74NAE+ /j0ku/LAkadGIgLz004V1JlUYyNXJSEB4TuUA3UAJJKskaYaeUkeNJW4NXc7DU1YM9cbwZc3P8XZGsinZtDWmW8h3n4yACdbDYJo7NNmAZnGyii/PJjqeZAx6bNnxjFSJsIEeU+N2meorT2JNPEuJwP0U8e4DKTX3m9rHtN3cp9ynx0mSSO/b /16Wr/G8LOjbjecgjpDi7bGMf9mx0DTCeOZrqGFUMsLvDb5BO33lBxZKDCPp47XodRp9ZhoIT3n5HBHWMynr+WUi67qonofier6ZqGduYqhHryfquRrrwby4W/ZQCr9+0zoUE2yXTf0cNnV6objZz6d4k22hbHuNW7jIL+8h25d3n+1LGPXog /hraqXQN75mdi+UaXKMRulROsBlXaD2mGcDqwYmfs3VMf2TbYRhCFoK1WnCkRp8qX67jbrgV/BpbawUjACV/MWfNvBgC+Qx+INHBBQWOIFj8Ga0XQhuoVi9X6c+Eq5EpJ6tdEPOmOMauHmjx97oMHmGwxrFcI3gGYncs5sa7sLrS6fUbowpx/ /Cj9ps1jerd9A76H+hvfyqzAxzTwG6cl8VZx5HJsVq2BZroDf5KIlJyw0xY6TvTye4q1BZdt9Z8IP7oIoK0NfqMd3XwppfODo+xp+KLfYyKsjvfb4Nyv3xx9T5bIZ97L6rmpJO3tWfX8+fpMWJe7f67HOPI8LILhUDws6vhpTpN8++h2A3+B0 /hqdk0Fhi0ODwKuXcgCeMHmBs0LvIsqqu1DF5yQS89+JwJ3oTYeAkQl0DwfKZq2Zmwh0pEoWGHtyHZeDDVjTXXEJVW0JcovUKm0iNc283cxh3pZoCpaGf/+i3jP4Mx9wOkSIJ3C1nXcbOem5Wsi7vvyLwlrgyjckS2yuOuA4RxmDAmN9805Qo
2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	{"event":{"provider":"Microsoft-Windows-PowerShell","kind":"event","code":"4104","created":"2022-02-19T20:12:55.522Z","action":"Execute a Remote Command"},"agent":{"hostname":"rdp0 {"kernel":"10.0.14393.4770 (rs1_release.211101-1440)","family":"windows","build":"14393.4770","version":"10.0","type":"windows","name":"Windows Server 2016 Datacenter","platform":"w text (11 of 56):\ntQBHAKfAS5c5F1wO+ozSN4YXHh47DqkOUJnYIa3B2taEyS+0rPzrXMH/KJB6nqar2+UfuDYfodlvnfKgaLs6sInCF7T/yt0WcxrCoFGpUKAqii4r+8xdZVkwgSQkET/cmclrXx3mQu7lLeJ4rDoDoz14tohDBb1iwaJ /KJOQNv5QS0sOpqq12AKtSi+EmgyqBOwLjidMQ8yg+qFVSL9y23qW0queBJ/G5ARVntglLP8sP7RFsF4j02Or59BuG43qHcBgLhH4u+LCgWpcS2zDN7XNRRfNG4qJI+5LZWbG/nHJgVoMR4za4tFRkBLmeAhMEyG8Ce+HavGuE7lzeoBrGaI/ /i4g4OxOwB4EUx0rDZM+P1jGwB25ynyStlDfs8mZ8sV7yhRJCAyHJZXMtkHTsD8ydxIa0uabc3sEv1pdlvInhEMTCIBWRkKtdDE6YViOaO3ns8EawjHMipT8CPcmyssm6/YZujaXhYrJhZY+TWRYlsugWBzTbucvfIBIUxFn0mXLmNkMfIIZH /A7JC9LwfkO5fSgVLytg5sYDbyYALlBHIhOLF62eUkiqPZvd0IfXE8exq52T+5fqW2qMHmftjymJBLfDDzALir9xmWfjcuJGH4DMUlpnbVf8x9hRcVpr+wvuSBbRjA/qvqOFMbNrlxUWjv5ha8+3G5F+UDNqUgHcjYctvxsSh9G7RND753Rt5 /vt53ALD0b7q93kCKulo92460Imb31iIYwI0m94eTbUCYTR+67V88xLF1aMzR88op4cqP3J+2+nE9iafws+9i0WJMC1GBp1MAj3G+WO01Tn0rzOor2nWzOr7Mpxi3SaPlgIw7pZovmhL+HLsUtXNRbBxDp19YPSbyzmnMJywGUxecaPiWEdSE /LGfEcPAfVTAA4YNtXXgpHygSWnbM8QVHMBskTyFLfVX7ibJttxiLvAYTRSNb4ndDiORcl327SsQfTVicY1TGTc9uABZAT7mzY4+4hkUxE2MkUSZayp3VLll9aUdho3dF9fO+Ik8fLr8WiRsY6jTbVXtLoFruqzHWTmr+wgd6v7aPS5BmiqYr

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:12 *to* 02/19/22 23:59

Splunk Search:

```
index=wineventlogs event.code=4104 _raw!="*ansible*"
 raw!="*amazon\.com*" _raw!="*EC2-Windows*"
 raw!="*NetworkPerformance*" | rex field= raw
"message\":\"(?<MessageExctracted>.+)" | eval
Message=MessageExctracted | rex mode=sed field=Message
"s/\\\n/*/g" | makemv delim="*",Message | rex mode=sed
field=Message "s/\\\t/*/g" | makemv delim="*",Message |
table _time index host.name event.code Message | sort _time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	Message

2022-02-19 20:12:55.522	wineventlogs	rdp01.magnumtempus.financial	4104	Creating Scriptblock text (1 of 56):
				function Invoke-BloodHound{
				    <#
				    .SYNOPSIS
				        Runs the BloodHound C# Ingestor using reflection. The assembly is stored in this file.
				    .DESCRIPTION
				        Using reflection and assembly.load, load the compiled BloodHound C# ingestor into memory
				        and run it without touching disk. Parameters are converted to the equivalent CLI arguments
				        for the SharpHound executable and passed in via reflection. The appropriate function
				        calls are made in order to ensure that assembly dependencies are loaded properly.
				    .PARAMETER CollectionMethod
				        Specifies the CollectionMethod being used. Possible value are:
				            Group - Collect group membership information
				            LocalGroup - Collect local group information for computers
				            LocalAdmin - Collect local admin users for computers
				            RDP - Collect remote desktop users for computers
				            DCOM - Collect distributed COM users for computers
				PSRemote - Collected members of the Remote Management Users group for computers
				            Session - Collect session information for computers
				            SessionLoop - Continuously collect session information until killed
				            Trusts - Enumerate domain trust data
				            ACL - Collect ACL (Access Control List) data
				            Container - Collect GPO/OU Data
				            ComputerOnly - Collects Local Admin and Session data
				            GPOLocalGroup - Collects Local Admin information using GPO (Group Policy Objects)
				            LoggedOn - Collects session information using privileged methods (needs admin!)
				            ObjectProps - Collects node property information for users and computers
				SPNTargets - Collects SPN targets (currently only MSSQL)
				            Default - Collects Group Membership, Local Admin, Sessions, and Domain Trusts
				            DcOnly - Collects Group Membership, ACLs, ObjectProps, Trusts, Containers, and GPO Admins
				            All - Collect all data except GPOLocalGroup
				        This can be a list of comma seperated valued as well to run multiple collection methods!
				.PARAMETER Stealth
				        Use stealth collection options, will sacrifice data quality in favor of much reduced
				        network impact
				    .PARAMETER Domain
				        Specifies the domain to enumerate. If not specified, will enumerate the current
				        domain your user context specifies.
				.PARAMETER WindowsOnly
				Limits computer collection to systems that have an operatingssytem attribute that matches

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:12:55 *to* 02/19/22 20:17:55

Splunk Search:

```
index=sysmon host.name="rdp01.magnumtempus.financial"
message!="*AppData*"
| table  time event.code message
| sort _time
```

SPLUNK: ENDPOINT LOGS

2022-02-19 20:12:56	22	Dns query: RuleName: - UtcTime: 2022-02-19 20:12:53.042 ProcessGuid: {B59E2A9A-4F1B-6211-8A01-000000001202} ProcessId: 6784 QueryName: raw.githubusercontent.com QueryStatus: 0 QueryResults: ::ffff:185.199.108.133;::ffff:185.199.109.133;::ffff:185.199.110.133;::ffff:185.199.111.133; Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: MAGNUMTEMPUS\pat.risus

SPLUNK: ENDPOINT LOGS

2022-02-19 20:13:08	24	Clipboard changed: RuleName: - UtcTime: 2022-02-19 20:13:06.037 ProcessGuid: {B59E2A9A-4F1B-6211-8A01-000000001202} ProcessId: 6784 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Session: 3 ClientInfo: user: MAGNUMTEMPUS\pat.risus hostname: hack Hashes: SHA1=DA39A3EE5E6B4B0D3255BFEF95601890AFD80709,MD5=D41D8CD98 Archived: true User: MAGNUMTEMPUS\pat.risus

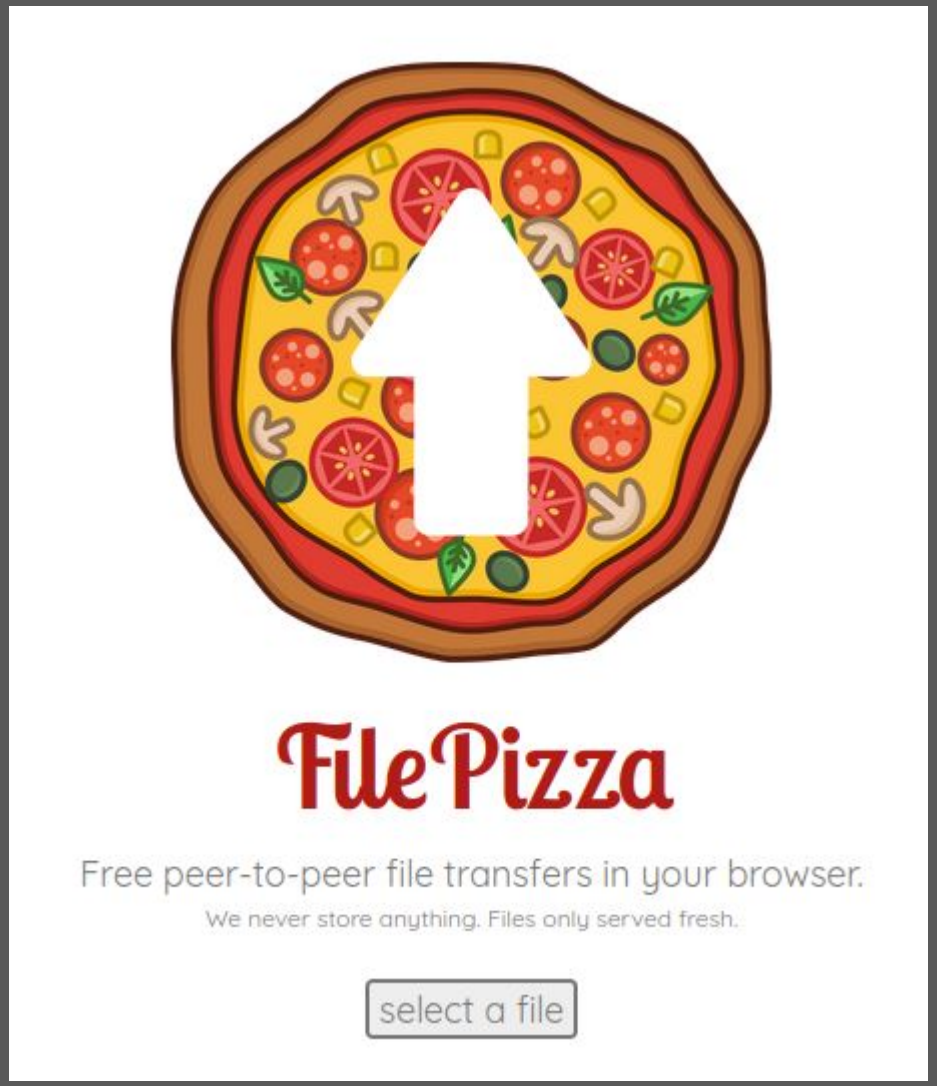
SPLUNK: ENDPOINT LOGS

```
2022-02-19 20:13:18    1    Process Create:
                            RuleName: technique_id=T1204,technique_name=User Execution
                            UtcTime: 2022-02-19 20:13:16.483
                            ProcessGuid: {B59E2A9A-4F5C-6211-A801-000000001202}
                            ProcessId: 6184
                            Image: C:\Program Files\Google\Chrome\Application\chrome.exe
                            FileVersion: 98.0.4758.102
                            Description: Google Chrome
                            Product: Google Chrome
                            Company: Google LLC
                            OriginalFileName: chrome.exe
                            CommandLine: "C:\Program Files\Google\Chrome\Application\chrome.exe"
                            CurrentDirectory: C:\Program Files\Google\Chrome\Application\
                            User: MAGNUMTEMPUS\pat.risus
                            LogonGuid: {B59E2A9A-4EE7-6211-D182-600000000000}
                            LogonId: 0x6082D1
                            TerminalSessionId: 3
                            IntegrityLevel: Medium
                            Hashes: SHA1=0608825F6B54238A452E3050D49E8AA50569A6C9,MD5=15150D9C89FEB4
                            ParentProcessGuid: {B59E2A9A-4EF6-6211-6B01-000000001202}
                            ParentProcessId: 5092
                            ParentImage: C:\Windows\explorer.exe
                            ParentCommandLine: C:\Windows\Explorer.EXE
                            ParentUser: MAGNUMTEMPUS\pat.risus
```

SPLUNK: ENDPOINT LOGS

```
2022-02-19 20:13:34        22    Dns query:
                                 RuleName: -
                                 UtcTime: 2022-02-19 20:13:31.806
                                 ProcessGuid: {B59E2A9A-4F60-6211-AB01-000000001202}
                                 ProcessId: 444
                                 QueryName: file.pizza
                                 QueryStatus: 0
                                 QueryResults: 104.21.15.118;172.67.162.149;
                                 Image: C:\Program Files\Google\Chrome\Application\chrome.exe
                                 User: MAGNUMTEMPUS\pat.risus
```

SPLUNK: ENDPOINT LOGS



Source: https://file.pizza/

SPLUNK: ENDPOINT LOGS

Exfiltration Over Web Service

Sub-techniques (2)

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services.

Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

ID: T1567

Sub-techniques: T1567.001, T1567.002

Tactic: Exfiltration

Platforms: Linux, Windows, macOS

Contributors: William Cain

Version: 1.1

Created: 09 March 2020

Last Modified: 15 October 2021

SPLUNK: ENDPOINT LOGS

```
2022-02-19 20:14:49          1    Process Create:
                                  RuleName: technique_id=T1016,technique_name=System Network Configuration Discovery
                                  UtcTime: 2022-02-19 20:14:47.070
                                  ProcessGuid: {B59E2A9A-4FB7-6211-E501-000000001202}
                                  ProcessId: 5164
                                  Image: C:\Windows\System32\ipconfig.exe
                                  FileVersion: 10.0.14393.0 (rs1_release.160715-1616)
                                  Description: IP Configuration Utility
                                  Product: Microsoft® Windows® Operating System
                                  Company: Microsoft Corporation
                                  OriginalFileName: ipconfig.exe
                                  CommandLine: "C:\Windows\system32\ipconfig.exe" /all
                                  CurrentDirectory: C:\Users\pat.risus\
                                  User: MAGNUMTEMPUS\pat.risus
                                  LogonGuid: {B59E2A9A-4EE7-6211-D182-600000000000}
                                  LogonId: 0x6082D1
                                  TerminalSessionId: 3
                                  IntegrityLevel: Medium
                                  Hashes: SHA1=A95BEAA8B81FD799DB6051A79D959908FFBDB22F,MD5=29916DCEA5377C19996B417D923
                                  ParentProcessGuid: {B59E2A9A-4F1B-6211-8A01-000000001202}
                                  ParentProcessId: 6784
                                  ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
                                  ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
                                  ParentUser: MAGNUMTEMPUS\pat.risus
```

Portscan

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:14:36 *to* 02/19/22 23:59:00

Splunk Search:

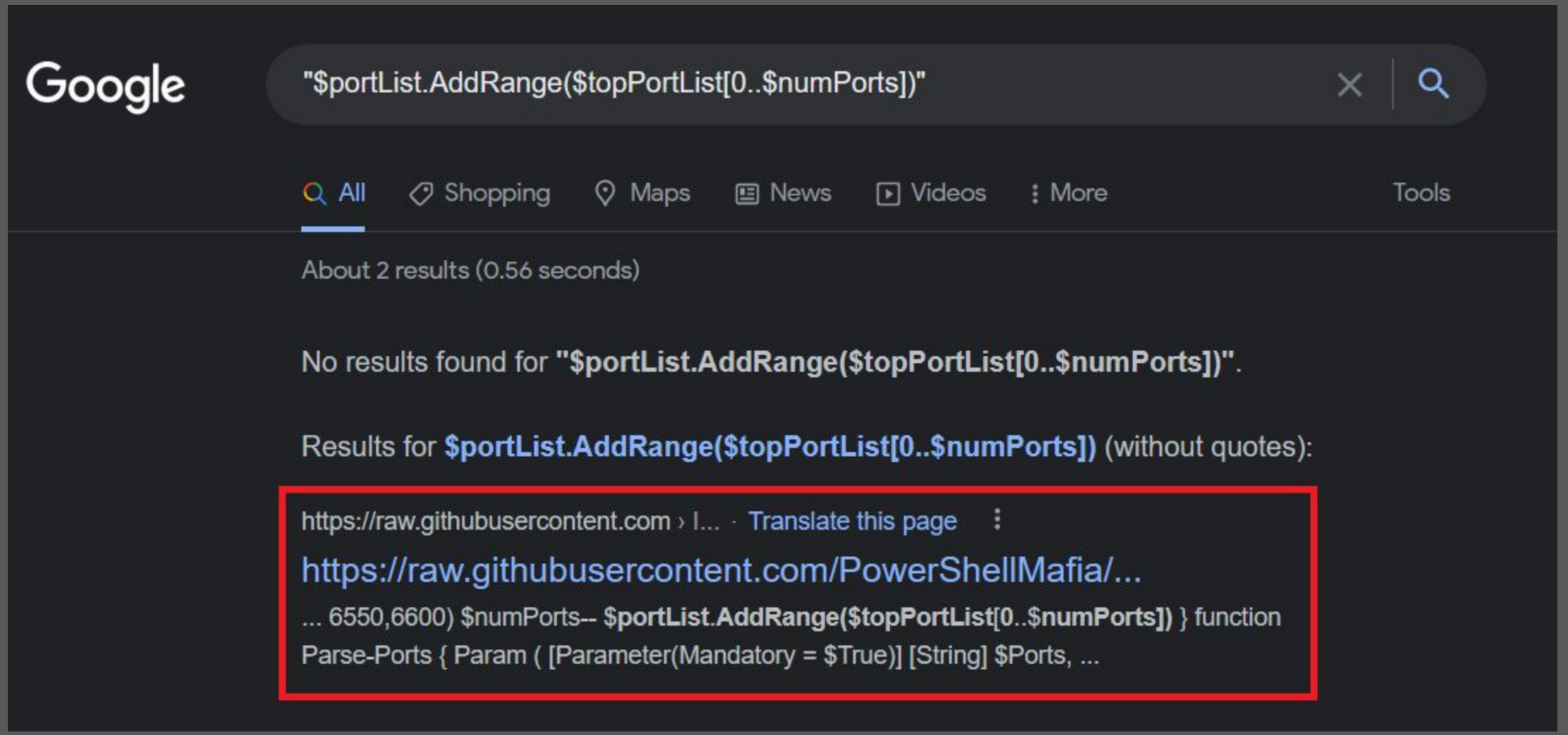
```
index=wineventlogs host.name="rdp01.magnumtempus.financial"
event.code=4104  raw!="*ansible*"  raw!="*amazon\.com*"
 raw!="*EC2-Windows*"  raw!="*NetworkPerformance*"
| rex field= raw "message\":\"(?<MessageExctracted>.+)"
| eval Message=MessageExctracted
| rex mode=sed field=Message "s/\\\n/*/g"
| makemv delim="*",Message
| rex mode=sed field=Message "s/\\\t/*/g"
| makemv delim="*",Message
| table  time index host.name event.code Message
| sort _time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	Message
2022-02-19 20:15:44.768	wineventlogs	rdp01.magnumtempus.financial	4104	Creating Scriptblock text (2 of 3):

```
971,1972,1974,2099,2170,2196,2200,2288,2366,2382,2557,2800,2910,2920,2968,3007,
                        3013,3050,3119,3304,3307,3376,3400,3410,3514,3684,3697,3700,3824,3846,3848,3859,
                        3863,3870,3872,3888,3907,3916,3931,3941,3957,3963,3968,3969,3972,3990,3993,3994,
                        4009,4040,4080,4096,4143,4147,4200,4252,4430,4555,4600,4658,4875,4949,5040,5063,
                        5074,5151,5212,5223,5242,5279,5339,5353,5501,5807,5812,5818,5823,5868,5869,5899,
                        5905,5909,5914,5918,5938,5940,5968,5981,6051,6060,6068,6203,6247,6500,6504,6520,
                        6550,6600)
    $numPorts--
    $portList.AddRange($topPortList[0..$numPorts])
}
function Parse-Ports
{
    Param (
        [Parameter(Mandatory = $True)] [String] $Ports,
        [Parameter(Mandatory = $True)] $pList
    )
    foreach ($pRange in $Ports.Split(\",\"))
    {
        #-1 is a special case for ping
        if ($pRange -eq \"-1\")
        {
            $pList.Add([int]$pRange)
        }
        elseif ($pRange.Contains(\"-\"))
        {
            [int[]] $range = $pRange.Split(\"-\")
            if ($range.Count -ne 2 -or $pRange.Split(\"-\")[0] -eq \"\" -or $pRange.split(\"-\")[1] -eq \"\")
            {
                throw \"Invalid port range\"
            }
            $pList.AddRange($range[0]..$range[1])
        }
        else
        {
            $pList.Add([int]$pRange)
        }
```

SPLUNK: ENDPOINT LOGS



SPLUNK: ENDPOINT LOGS

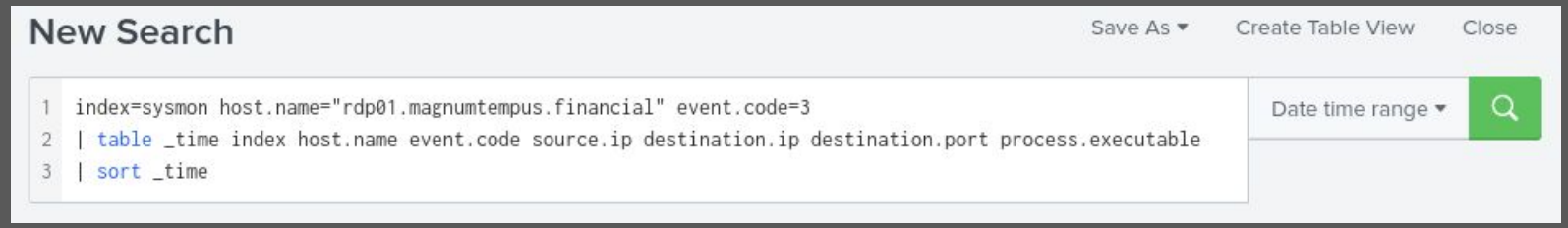
```
function Invoke-Portscan
{
<#
.SYNOPSIS

Simple portscan module

PowerSploit Function: Invoke-Portscan
Author: Rich Lundeen (http://webstersProdigy.net)
License: BSD 3-Clause
Required Dependencies: None
Optional Dependencies: None

.DESCRIPTION

Does a simple port scan using regular sockets, based (pretty) loosely on nmap

.PARAMETER Hosts

Include these comma seperated hosts (supports IPv4 CIDR notation) or pipe them in

.PARAMETER HostFile

Input hosts from file rather than commandline
```

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:15:44 *to* 02/19/22 20:25:44

Splunk Search:

```
index=sysmon host.name="rdp01.magnumtempus.financial"
event.code=3
| table  time index host.name event.code source.ip destination.ip
destination.port process.executable
| sort  _time
```



SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	source.ip	destination.ip	destination.port	process.executable
2022-02-19 20:15:48	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	185.199.108.133	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:17:40	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	20.189.173.6	443	C:\Users\pat.risus\AppData\Local\Microsoft\Teams\current\Teams.exe
2022-02-19 20:17:42	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.100	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:17:45	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.101	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:17:50	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.110	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:17:58	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.130	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:17:59	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.131	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:01	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.133	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:01	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.132	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:03	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.134	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:04	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.136	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:04	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.135	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:04	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.138	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:04	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.137	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:08	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.144	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:08	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.141	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:08	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.143	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:08	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.142	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:18:08	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	172.16.50.139	445	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-02-19 20:21:38	sysmon	rdp01.magnumtempus.financial	3	172.16.55.110	185.199.108.133	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
source.ip:172.16.55.110 AND NOT destination.port:(4789 OR 443 OR 53) |
groupby destination.port
```

SECURITY ONION: NETWORK LOGS

Count ▼	destination.port
6,643	445
482	135
189	88
184	80
139	49679
115	49666
79	5044
64	389

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
source.ip:172.16.55.110 AND destination.port:(445 OR 389 OR 135 OR 88
) | groupby destination.ip
```

SECURITY ONION: NETWORK LOGS

Count	destination.ip ▲
5	172.16.43.7
1	172.16.50.10
703	172.16.50.100
529	172.16.50.101
632	172.16.50.110
427	172.16.50.130
404	172.16.50.131
403	172.16.50.132
403	172.16.50.133
360	172.16.50.134
358	172.16.50.135
345	172.16.50.136
368	172.16.50.137
331	172.16.50.138
334	172.16.50.139
379	172.16.50.140
354	172.16.50.141
342	172.16.50.142
366	172.16.50.143
380	172.16.50.144
1	18.188.230.95

SECURITY ONION: NETWORK LOGS

41	172.16.50.100	SF
10	172.16.50.110	SF
57	172.16.50.101	SF
7	172.16.50.130	SF
7	172.16.50.131	SF
7	172.16.50.132	SF
4	172.16.50.133	SF
1	172.16.50.140	SF
4	172.16.50.137	SF
4	172.16.50.134	SF
4	172.16.50.135	SF
1	172.16.50.141	SF
4	172.16.50.136	SF
1	172.16.50.139	SF
4	172.16.50.138	SF
1	18.188.230.95	SF
17	172.16.50.100	S1
5	172.16.43.7	S0
1	172.16.50.10	S0
100	172.16.50.100	RSTR
2	172.16.50.110	RSTR
12	172.16.50.101	RSTR
1	172.16.50.130	RSTR
1	172.16.50.131	RSTR
1	172.16.50.132	RSTR
1	172.16.50.133	RSTR
1	172.16.50.144	RSTR
1	172.16.50.140	RSTR
1	172.16.50.137	RSTR
1	172.16.50.143	RSTR
1	172.16.50.134	RSTR

SECURITY ONION: NETWORK LOGS

2022-02-19 20:08:30.584 +00:00	172.16.55.110	52911	172.16.50.101	389	udp	
2022-02-19 20:08:30.694 +00:00	172.16.55.110	49887	172.16.50.101	135	tcp	dce_rpc
2022-02-19 20:08:30.694 +00:00	172.16.55.110	49888	172.16.50.101	135	tcp	dce_rpc
2022-02-19 20:08:30.695 +00:00	172.16.55.110	49887	172.16.50.101	135		
2022-02-19 20:08:30.695 +00:00	172.16.55.110	49888	172.16.50.101	135		
2022-02-19 20:08:30.695 +00:00	172.16.55.110	49887	172.16.50.101	135		
2022-02-19 20:08:30.695 +00:00	172.16.55.110	49889	172.16.50.101	135	tcp	dce_rpc
2022-02-19 20:08:30.695 +00:00	172.16.55.110	49890	172.16.50.101	135	tcp	dce_rpc
2022-02-19 20:08:30.696 +00:00	172.16.55.110	49889	172.16.50.101	135		
2022-02-19 20:08:30.696 +00:00	172.16.55.110	49890	172.16.50.101	135		
2022-02-19 20:08:30.696 +00:00	172.16.55.110	49890	172.16.50.101	135		
2022-02-19 20:11:19.224 +00:00	172.16.55.110	51687	172.16.50.100	389	udp	
2022-02-19 20:11:19.413 +00:00	172.16.55.110	49912	172.16.50.101	135	tcp	dce_rpc
2022-02-19 20:11:19.413 +00:00	172.16.55.110	49912	172.16.50.101	135	tcp	dce_rpc

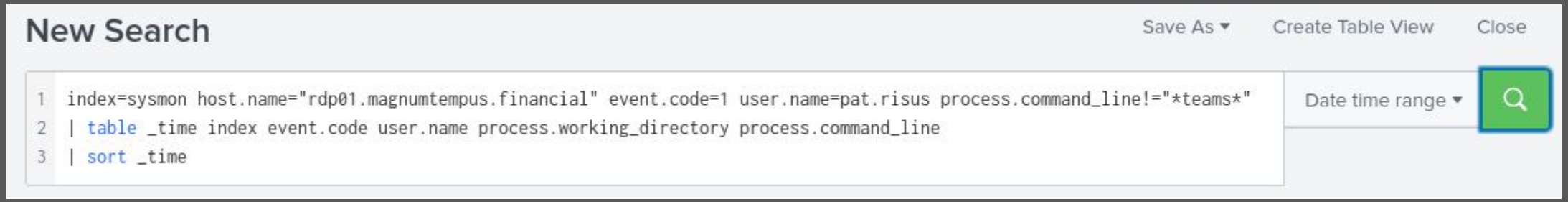
Kerberoasting

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:18:08 *to* 02/19/22 20:28:08

Splunk Search:

```
index=sysmon host.name="rdp01.magnumtempus.financial"
event.code=1 user.name=pat.risus process.command_line!="*teams*"
| table  time index event.code user.name
process.working_directory process.command_line
| sort  _time
```



SPLUNK: ENDPOINT LOGS

_time	index	event.code	user.name	process.working_directory	process.command_line
2022-02-19 20:18:08	sysmon	1	pat.risus	C:\Users\pat.risus\	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile
2022-02-19 20:18:08	sysmon	1	pat.risus	C:\Users\pat.risus\	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile
2022-02-19 20:18:08	sysmon	1	pat.risus	C:\Users\pat.risus\	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile
2022-02-19 20:18:08	sysmon	1	pat.risus	C:\Users\pat.risus\	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile
2022-02-19 20:18:08	sysmon	1	pat.risus	C:\Users\pat.risus\	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile
2022-02-19 20:18:08	sysmon	1	pat.risus	C:\Users\pat.risus\	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile
2022-02-19 20:18:11	sysmon	1	pat.risus	C:\Users\pat.risus\	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile
2022-02-19 20:18:11	sysmon	1	pat.risus	C:\Users\pat.risus\	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Version 5.1 -s

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:18:08 to 02/19/22 20:28:08

Splunk Search:

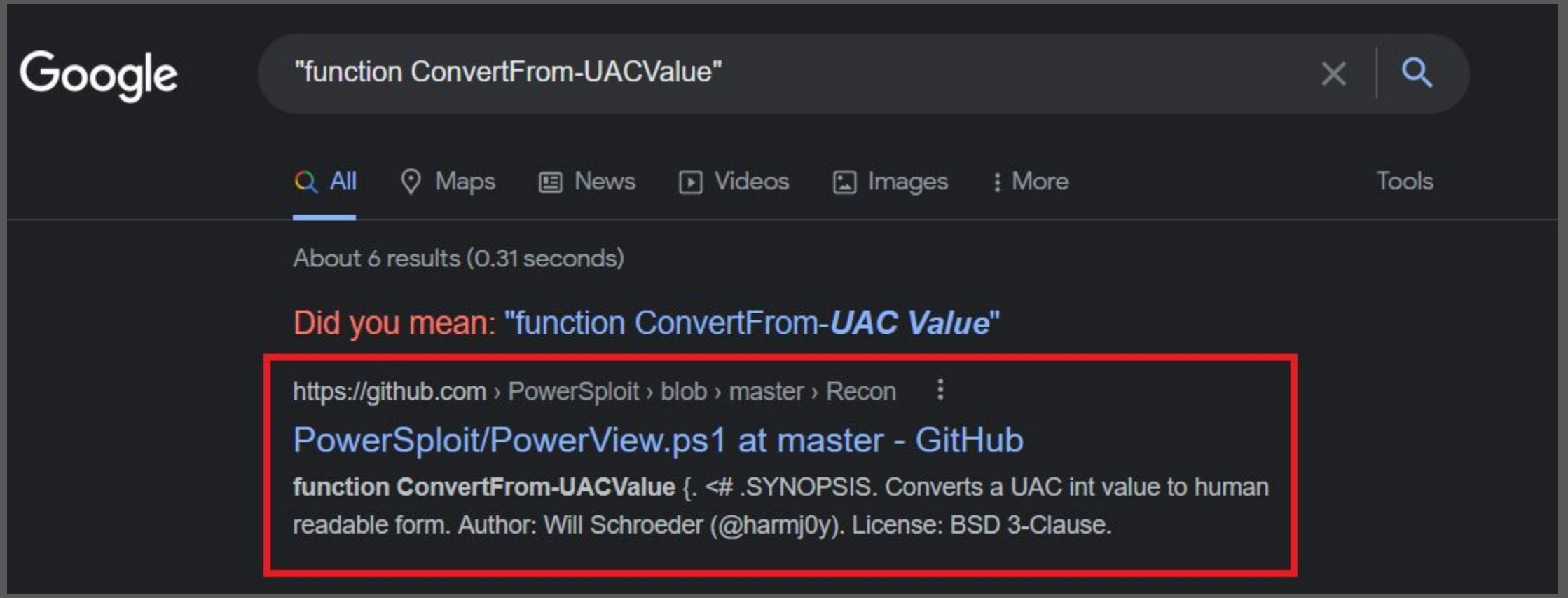
```
index=wineventlogs host.name="rdp01.magnumtempus.financial"
event.code=4104  raw!="*ansible*"  raw!="*amazon\.com*"
 raw!="*EC2-Windows*"  raw!="*NetworkPerformance*"
| rex field=_raw "message\":\"(?<MessageExctracted>.+)"
| eval Message=MessageExctracted
| rex mode=sed field=Message "s/\\\n/*/g"
| makemv delim="*",Message
| rex mode=sed field=Message "s/\\\t/*/g"
| makemv delim="*",Message
| table _time index host.name event.code Message
| sort _time
```

SPLUNK: ENDPOINT LOGS

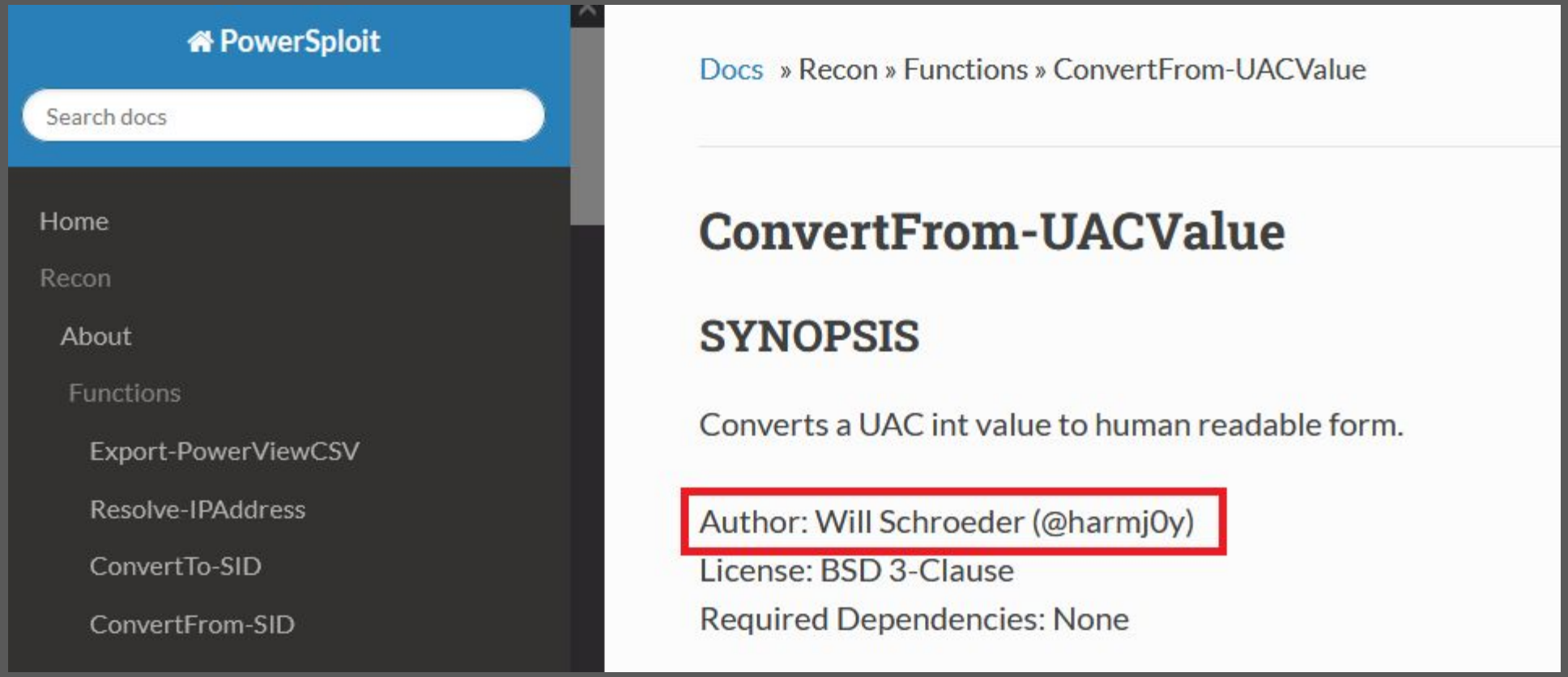
_time	index	host.name	event.code	Message

2022-02-19 20:21:37.161	wineventlogs	rdp01.magnumtempus.financial	4104	Creating Scriptblock text (4 of 30):
				e -replace \"/\",\"\\\"
				    # Accessor functions to simplify calls to NameTranslate
				    function Invoke-Method([__ComObject] $object, [String] $method, $parameters) {
				        $output = $object.GetType().InvokeMember($method, \"InvokeMethod\", $NULL, $object, $parameters)
				        if ($output) { $output }
				    }
				    function Set-Property([__ComObject] $object, [String] $property, $parameters) {
				        [Void] $object.GetType().InvokeMember($property, \"SetProperty\", $NULL, $object, $parameters)
				    }
				    $Translate = New-Object -comobject NameTranslate
				    try {
				        Invoke-Method $Translate \"Init\" (1, $Domain)
				    }
				    catch [System.Management.Automation.MethodInvocationException] { }
				    Set-Property $Translate \"ChaseReferral\" (0x60)
				    try {
				        Invoke-Method $Translate \"Set\" (5, $ObjectName)
				        (Invoke-Method $Translate \"Get\" (3))
				    }
				    catch [System.Management.Automation.MethodInvocationException] { $_ }
				}
				function ConvertFrom-UACValue {
				<#
				    .SYNOPSIS
				        Converts a UAC int value to human readable form.
				    .PARAMETER Value
				        The int UAC value to convert.
				    .PARAMETER ShowAll
				        Show all UAC values, with a + indicating the value is currently set.
				    .EXAMPLE
				        PS C:\\> ConvertFrom-UACValue -Value 66176
				        Convert the UAC value 66176 to human readable format.
				    .EXAMPLE
				        PS C:\\> Get-NetUser jason | select useraccountcontrol | ConvertFrom-UACValue
				        Convert the UAC value for 'jason' to human readable format.
				    .EXAMPLE

SPLUNK: ENDPOINT LOGS



SPLUNK: ENDPOINT LOGS



Source: https://powersploit.readthedocs.io/en/latest/Recon/ConvertFrom-UACValue/

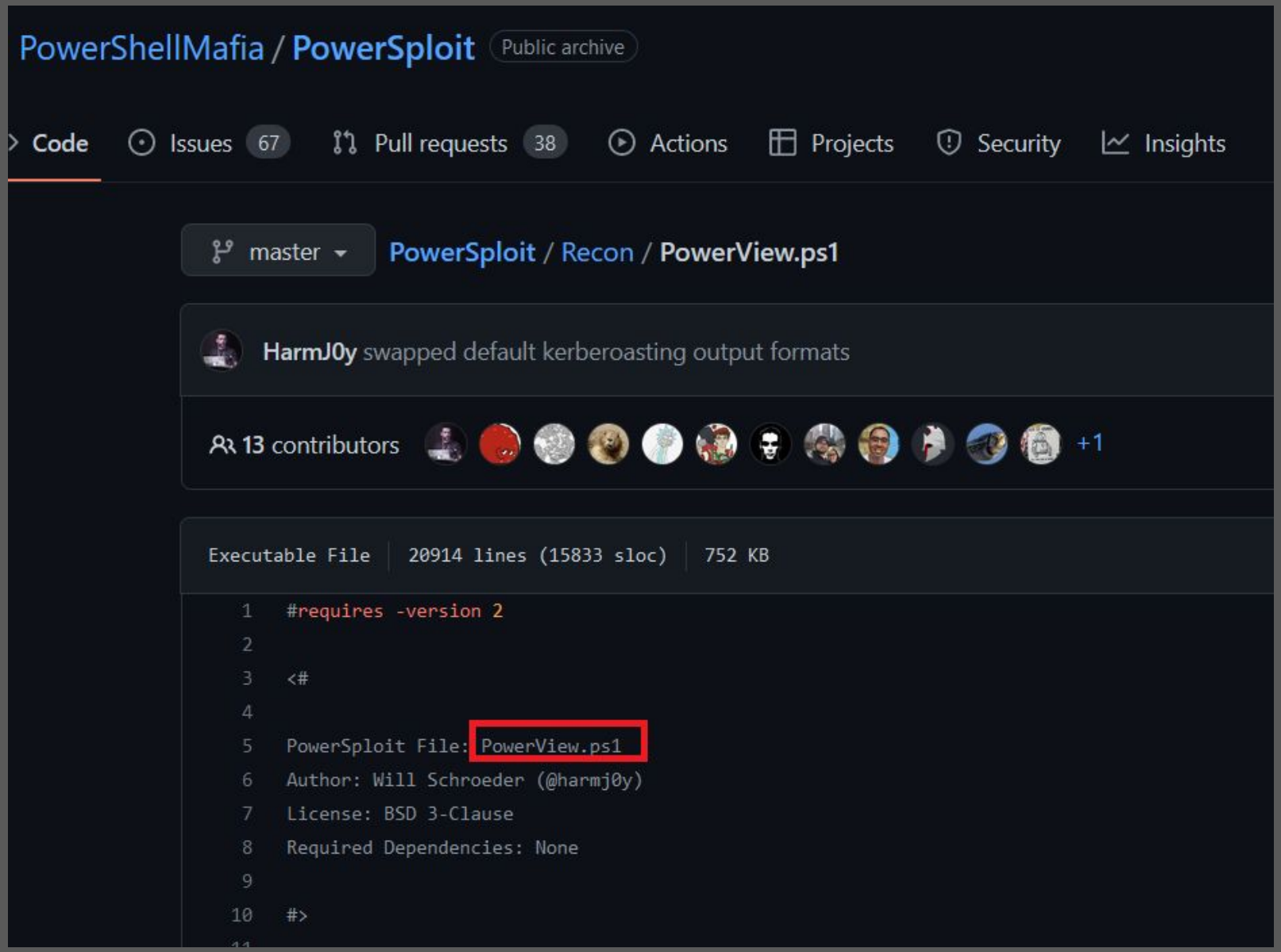
SPLUNK: ENDPOINT LOGS

Image Source: Meme created

SPLUNK: ENDPOINT LOGS

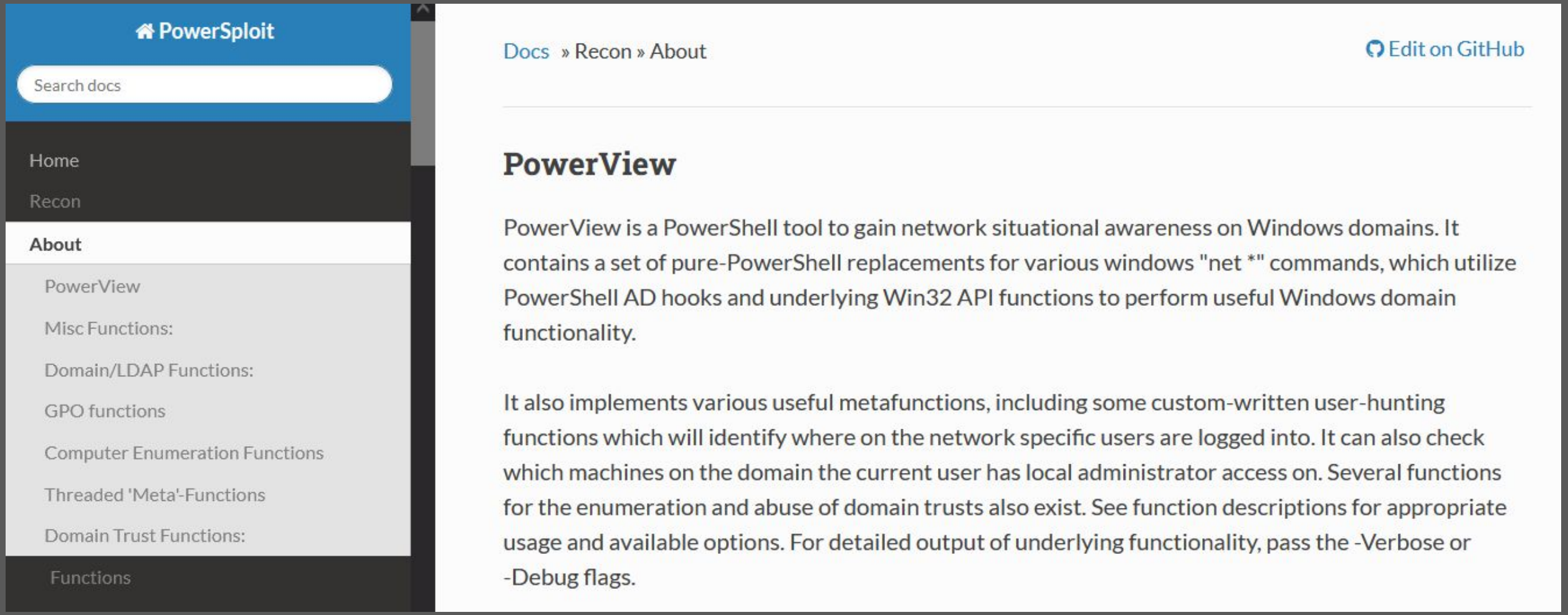
_time	index	host.name	event.code	Message
2022-02-19 20:21:37.161	wineventlogs	rdp01.magnumtempus.financial	4104	Creating Scriptblock text (1 of 30): #requires -version 2 <# PowerSploit File: PowerView.ps1 Author: Will Schroeder (@harmj0y) License: BSD 3-Clause Required Dependencies: None Optional Dependencies: None #> ## # # PSReflect code for Windows API access # Author: @mattifestation # https://raw.githubusercontent.com/mattifestation/PSReflect/master/PSReflect.psm1 # ## function New-InMemoryModule { <# .SYNOPSIS Creates an in-memory assembly and module Author: Matthew Graeber (@mattifestation) License: BSD 3-Clause Required Dependencies: None Optional Dependencies: None .DESCRIPTION When defining custom enums, structs, and unmanaged functions, it is necessary to associate to an assembly module. This helper function creates an in-memory module that can be passed to the 'enum', 'struct', and Add-Win32Type functions. .PARAMETER ModuleName Specifies the desired name for the in-memory assembly and module. If ModuleName is not provided, it will default to a GUID. .EXAMPLE $Module = New-InMemoryModule -ModuleName Win32 #> Param ([Parameter(Position = 0)] [ValidateNotNullOrEmpty()] [String]

SPLUNK: ENDPOINT LOGS



Source: https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

SPLUNK: ENDPOINT LOGS



Source: https://powersploit.readthedocs.io/en/latest/Recon/

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	Message
2022-02-19 20:22:03.221	wineventlogs	rdp01.magnumtempus.financial	4104	Creating Scriptblock text (1 of 4): <# Kerberoast.ps1 Author: Will Schroeder (@harmj0y) License: BSD 3-Clause Required Dependencies: None Note: the primary method of use will be Invoke-Kerberoast with various targeting options. #> function Get-DomainSearcher {

SPLUNK: ENDPOINT LOGS

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

SPLUNK: ENDPOINT LOGS

Steal or Forge Kerberos Tickets: Kerberoasting

Other sub-techniques of Steal or Forge Kerberos Tickets (4)

Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force.[1][2]

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service[3]).[4][5][6][7]

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC).[1][2] Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline Brute Force attacks that may expose plaintext credentials.[2][1] [7]

This same behavior could be executed using service tickets captured from network traffic.[2]

ID: T1558.003

Sub-technique of: T1558

ⓘ Tactic: Credential Access

ⓘ Platforms: Windows

ⓘ System Requirements: Valid domain account or the ability to sniff traffic within a domain

ⓘ CAPEC ID: CAPEC-509

Contributors: Praetorian

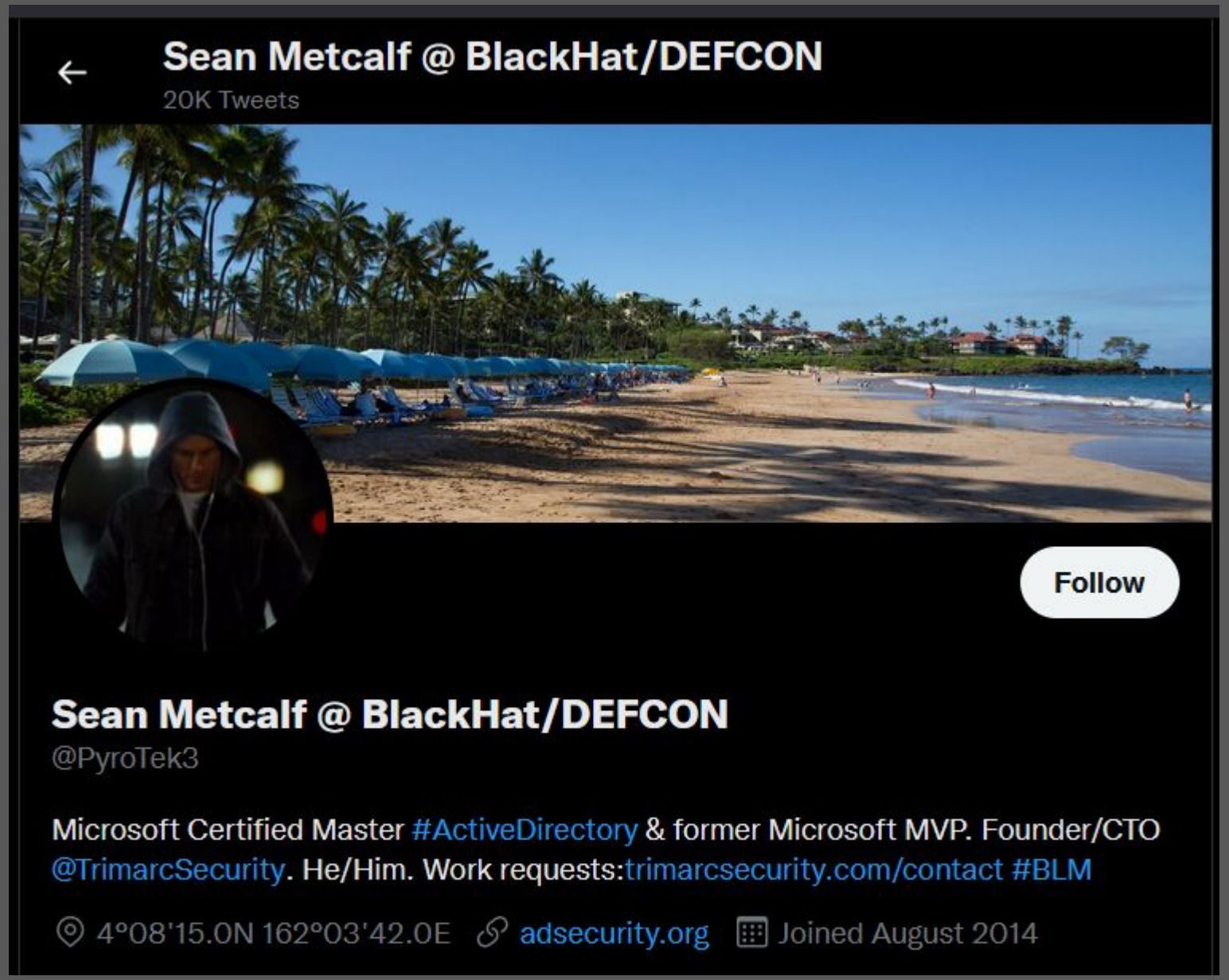
Version: 1.2

Created: 11 February 2020

Last Modified: 08 March 2022

Version Permalink

SPLUNK: ENDPOINT LOGS



SPLUNK: ENDPOINT LOGS

FEB
05
2017

Detecting Kerberoasting Activity

By Sean Metcalf in ActiveDirectorySecurity, Hacking, Microsoft Security, Technical Reference

Introduction

Kerberoasting can be an effective method for extracting service account credentials from Active Directory as a regular user without sending any packets to the target system. This attack is effective since people tend to create poor passwords. The reason why this attack is successful is that most service account passwords are the same length as the domain password minimum (often 10 or 12 characters long) meaning that even brute force cracking doesn't likely take longer than the password maximum password age (expiration). Most service accounts don't have passwords set to expire, so it's likely the same password will be in effect for months if not years. Furthermore, most service accounts are over-permissioned and are often members of Domain Admins providing full admin rights to Active Directory (even

SPLUNK: ENDPOINT LOGS

These events can be filtered using the following which greatly reduces the amount of events flowing into the SIEM/Splunk:

- Ticket Options: 0x40810000
- Ticket Encryption: 0x17

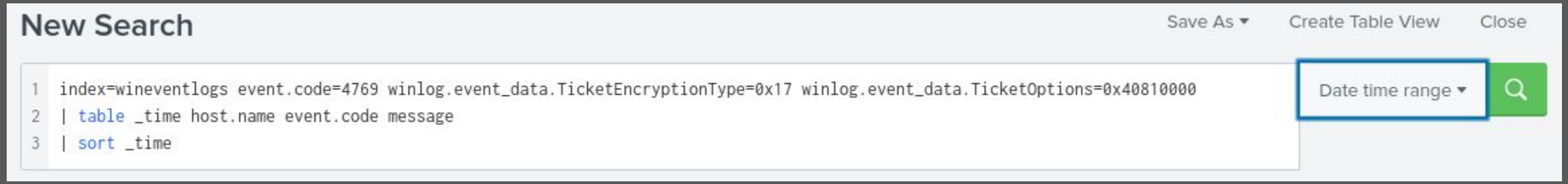
With this information, we can start investigating potential Kerberoasting activity and reduce the number of 4769 events.

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:21:00 *to* 02/19/22 20:23:00

Splunk Search:

```
index=wineventlogs event.code=4769
winlog.event_data.TicketEncryptionType=0x17
winlog.event_data.TicketOptions=0x40810000
| table  _time host.name event.code message
| sort _time
```



SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	message
2022-02-19 20:21:39.328	dc.magnumtempus.financial	4769	A Kerberos service ticket was requested. Account Information: Account Name: pat.risus@MAGNUMTEMPUS.FINANCIAL Account Domain: MAGNUMTEMPUS.FINANCIAL Logon GUID: {A1B60E3C-2456-8A5D-9260-81F7FCDC80E0} Service Information: Service Name: brent.socium Service ID: S-1-5-21-2370586174-1517003462-1142029260-1156 Network Information: Client Address: ::ffff:172.16.55.110 Client Port: 50843 Additional Information: Ticket Options: 0x40810000 Ticket Encryption Type: 0x17 Failure Code: 0x0 Transited Services: -

SPLUNK: ENDPOINT LOGS

2022-02-19 20:22:04.483 dc.magnumtempus.financial 4769 A Kerberos service ticket was requested.

Account Information:
- Account Name: pat.risus@MAGNUMTEMPUS.FINANCIAL
- Account Domain: MAGNUMTEMPUS.FINANCIAL
- Logon GUID: {87838BA7-8AF8-A642-158A-768EC79FB558}

Service Information:
- Service Name: reggie.habeo
- Service ID: S-1-5-21-2370586174-1517003462-1142029260-1138

Network Information:
- Client Address: ::ffff:172.16.55.110
- Client Port: 50876

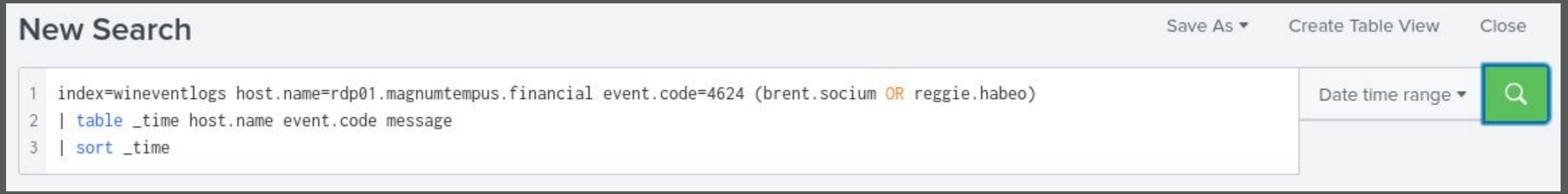
Additional Information:
- Ticket Options: 0x40810000
- Ticket Encryption Type: 0x17
- Failure Code: 0x0
- Transited Services: -

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:21:00 *to* 02/19/22 20:23:00

Splunk Search:

```
index=wineventlogs host.name=rdp01.magnumtempus.financial
event.code=4624 (brent.socium OR reggie.habeo)
| table  time host.name event.code message
| sort _time
```



SPLUNK: ENDPOINT LOGS

_time	host.name	event.code	message
2022-02-19 20:32:31.866	rdp01.magnumtempus.financial	4624	An account was successfully logged on. Subject: Security ID: S-1-5-21-2370586174-1517003462-1142029260-1171 Account Name: pat.risus Account Domain: MAGNUMTEMPUS Logon ID: 0x6060A6 Logon Information: Logon Type: 2 Restricted Admin Mode: - Virtual Account: No Elevated Token: No Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-2370586174-1517003462-1142029260-1156 Account Name: brent.socium Account Domain: MAGNUMTEMPUS Logon ID: 0x9F172E Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {43D63B85-E058-1E37-8AF8-4E01EB3DE82A} Process Information: Process ID: 0x2a0 Process Name: C:\Windows\System32\svchost.exe Network Information: Workstation Name: RDP01 Source Network Address: ::1 Source Port: 0 Detailed Authentication Information: Logon Process: seclogo Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:32:30 *to* 02/19/22 20:23:00

Splunk Search:

```
index=sysmon host.name="rdp01.magnumtempus.financial"
event.code=1 process.command_line!="*teams*"
| rename process.command_line as CommandLine
| table  _time index host.name event.code user.name CommandLine
| sort _time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	user.name	CommandLine
2022-02-19 20:32:38	sysmon	rdp01.magnumtempus.financial	1	brent.socium	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
2022-02-19 20:32:38	sysmon	rdp01.magnumtempus.financial	1	brent.socium	"C:\Windows\system32\RunDll32.exe" C:\Windows\System32 \shell32.dll,RunAsNewUser_RunDLL Local\{4ddb9f3f-700c-4bd6-9fc0-eaf85c01d25b}.00001cc4
2022-02-19 20:36:28	sysmon	rdp01.magnumtempus.financial	1	brent.socium	"C:\Windows\system32\PING.EXE" files.magnumtempus.finacial
2022-02-19 20:36:57	sysmon	rdp01.magnumtempus.financial	1	pat.risus	C:\Windows\System32\rundll32.exe C:\Windows\System32 \shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding
2022-02-19 20:37:34	sysmon	rdp01.magnumtempus.financial	1	brent.socium	"C:\Windows\system32\PING.EXE" files.magnumtempusfinancial.com
2022-02-19 20:37:57	sysmon	rdp01.magnumtempus.financial	1	NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:32:30 *to* 02/19/22 20:42:00

Splunk Search:

```
index=wineventlogs host.name="files.magnumtempus.financial"
event.code=4624 (RDP01 OR brent.socium OR 172.16.55.110)
| table  time index host.name event.code user.name message
| sort  _time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	user.name	message
2022-02-19 20:32:36.779	wineventlogs	files.magnumtempus.financial	4624		An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Information: Logon Type: 3 Restricted Admin Mode: - Virtual Account: No Elevated Token: No Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-2370586174-1517003462-1142029260-1156 Account Name: brent.socium Account Domain: MAGNUMTEMPUS Logon ID: 0x2B5651 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {00000000-0000-0000-0000-000000000000} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: RDP01 Source Network Address: 172.16.55.110 Source Port: 49802 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): NTLM V1

SPLUNK: ENDPOINT LOGS

Remote Services: SMB/Windows Admin Shares

Other sub-techniques of Remote Services (6)

Adversaries may use Valid Accounts to interact with a remote network share using Server Message Block (SMB). The adversary may then perform actions as the logged-on user.

SMB is a file, printer, and serial port sharing protocol for Windows machines on the same network or domain. Adversaries may use SMB to interact with file shares, allowing them to move laterally throughout a network. Linux and macOS implementations of SMB typically use Samba.

Windows systems have hidden network shares that are accessible only to administrators and provide the ability for remote file copy and other administrative functions. Example network shares include `C$`, `ADMIN$`, and `IPC$`. Adversaries may use this technique in conjunction with administrator-level Valid Accounts to remotely access a networked system over SMB,[1] to interact with systems using remote procedure calls (RPCs),[2] transfer files, and run transferred binaries through remote Execution. Example execution techniques that rely on authenticated sessions over SMB/RPC are Scheduled Task/Job, Service Execution, and Windows Management Instrumentation. Adversaries can also use NTLM hashes to access administrator shares on systems with Pass the Hash and certain configuration and patch levels.[3]

ID: T1021.002

Sub-technique of: T1021

Tactic: Lateral Movement

Platforms: Windows

System Requirements: SMB enabled; Host/network firewalls not blocking SMB ports between source and destination; Use of domain account in administrator group on remote system or default system admin account.

Permissions Required: Administrator, User

CAPEC ID: CAPEC-561

Version: 1.0

Created: 11 February 2020

Last Modified: 23 March 2020

Source: https://attack.mitre.org/techniques/T1021/002/

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:36:28 *to* 02/19/22 20:46:00

Splunk Search:

```
index=sysmon host.name="rdp01.magnumtempus.financial"
(event.code=1 OR event.code=22) _raw!="*Teams*"
| rename "dns.resolved_ip{}" as IP
| eval Info=mvappend('process.command_line','dns.question.name')
| mvexpand Info
| table _time index host.name event.code process.name Info IP
| sort _time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	process.name	Info	IP
2022-02-19 20:36:28	sysmon	rdp01.magnumtempus.financial	1	PING.EXE	"C:\Windows\system32\PING.EXE" files.magnumtempus.finacial	
2022-02-19 20:36:30	sysmon	rdp01.magnumtempus.financial	22	<unknown process>	files.magnumtempus.finacial	
2022-02-19 20:36:57	sysmon	rdp01.magnumtempus.financial	1	rundll32.exe	C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding	
2022-02-19 20:37:34	sysmon	rdp01.magnumtempus.financial	1	PING.EXE	"C:\Windows\system32\PING.EXE" files.magnumtempusfinancial.com	
2022-02-19 20:37:37	sysmon	rdp01.magnumtempus.financial	22	<unknown process>	files.magnumtempusfinancial.com	172.16.50.110
2022-02-19 20:37:57	sysmon	rdp01.magnumtempus.financial	1	WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	
2022-02-19 20:38:00	sysmon	rdp01.magnumtempus.financial	22	svchost.exe	files.magnumtempusfinacial.com	
2022-02-19 20:41:32	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	lh5.googleusercontent.com	142.250.190.65
2022-02-19 20:41:32	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	www.google.com	142.250.190.68
2022-02-19 20:41:35	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	interact.sh	46.101.25.250

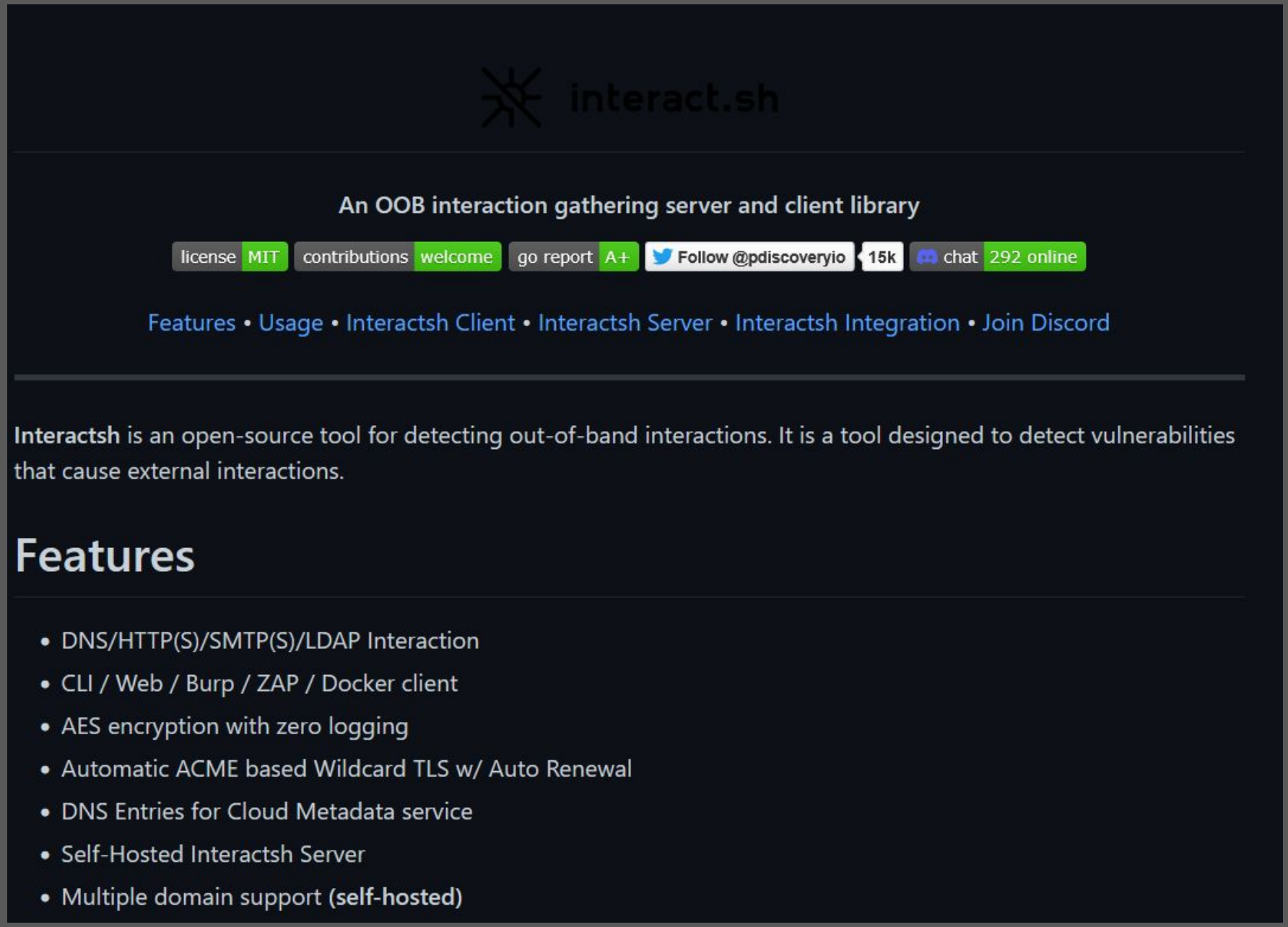
SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	process.name	Info	IP
2022-02-19 20:41:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	collector.github.com	140.82.113.21
2022-02-19 20:41:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	content-autofill.googleapis.com	172.217.0.170
2022-02-19 20:41:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	user-images.githubusercontent.com	185.199.111.133 185.199.110.133 185.199.109.133 185.199.108.133
2022-02-19 20:41:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	github-cloud.s3.amazonaws.com	52.217.138.17
2022-02-19 20:41:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	avatars.githubusercontent.com	185.199.111.133 185.199.108.133 185.199.109.133 185.199.110.133
2022-02-19 20:41:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	github.githubassets.com	185.199.108.154 185.199.109.154 185.199.110.154 185.199.111.154
2022-02-19 20:41:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	github.com	140.82.114.4
2022-02-19 20:41:41	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	api.github.com	140.82.114.6
2022-02-19 20:42:01	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	app.interactsh.com	104.26.9.171 172.67.71.174 104.26.8.171
2022-02-19 20:42:01	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	interactsh.com	172.67.71.174 104.26.9.171 104.26.8.171

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	process.name	Info	IP
2022-02-19 20:42:03	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	hits-i.iubenda.com	161.35.91.33 46.101.133.82 46.101.132.18 64.225.68.135 178.62.192.243 138.68.91.103
2022-02-19 20:42:03	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	www.iubenda.com	23.73.250.190
2022-02-19 20:42:03	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	cdn.iubenda.com	23.73.250.190
2022-02-19 20:43:12	sysmon	rdp01.magnumtempus.financial	22	powershell.exe	c88nc6r2vtc00001pg0ggrrksdcyyyyyb.interact.sh	46.101.25.250
2022-02-19 20:43:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	play.google.com	142.250.191.238
2022-02-19 20:43:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	apis.google.com	172.217.2.46
2022-02-19 20:43:39	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	id.google.com	142.250.191.163
2022-02-19 20:43:46	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	content-autofill.googleapis.com	142.250.191.234
2022-02-19 20:43:46	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	webwormhole.io	213.188.195.230
2022-02-19 20:44:12	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	relay.webwormhole.io.	157.245.15.73

SPLUNK: ENDPOINT LOGS



interact.sh

An OOB interaction gathering server and client library

license MIT | contributions welcome | go report A+ | Follow @pdiscoveryio 15k | chat 292 online

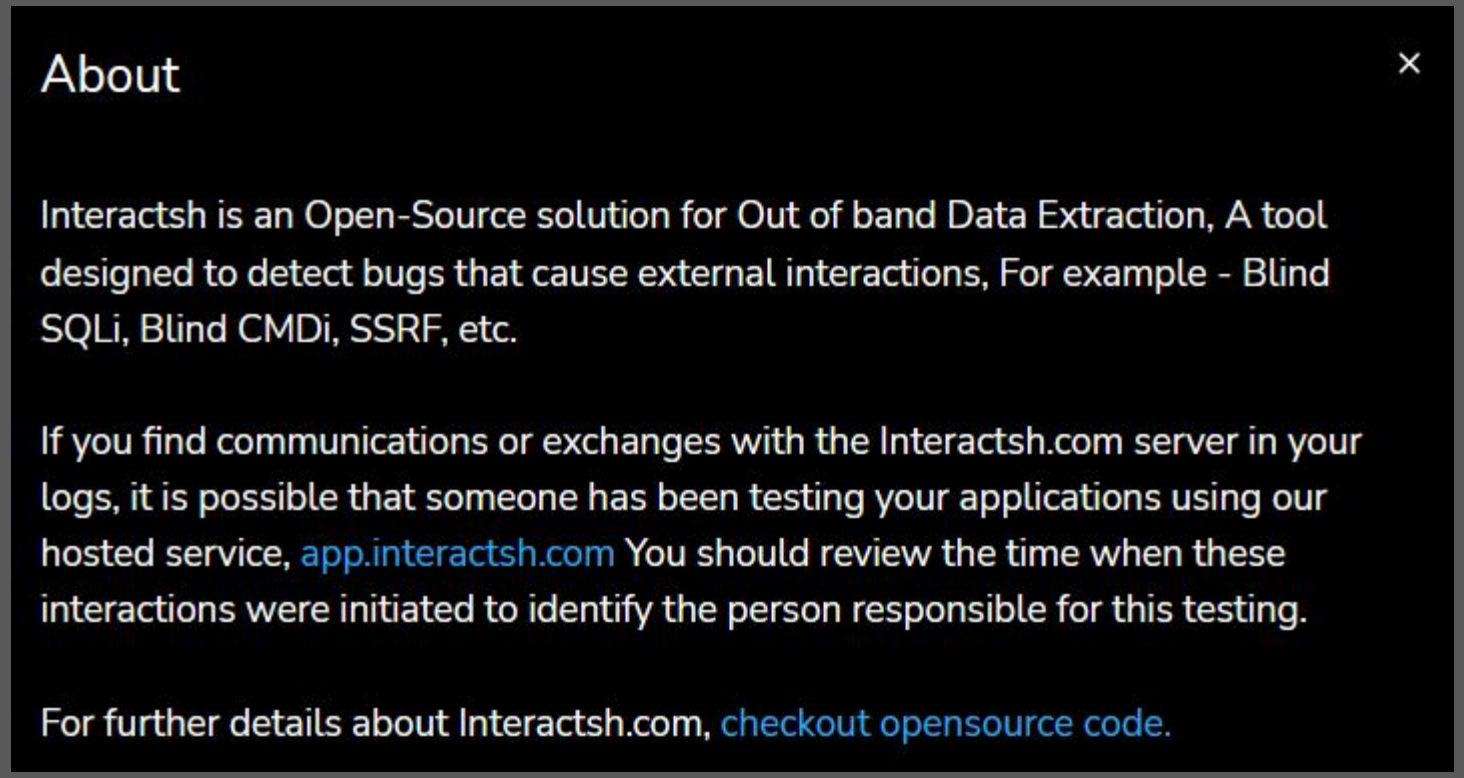
Features • Usage • Interactsh Client • Interactsh Server • Interactsh Integration • Join Discord

Interactsh is an open-source tool for detecting out-of-band interactions. It is a tool designed to detect vulnerabilities that cause external interactions.

Features

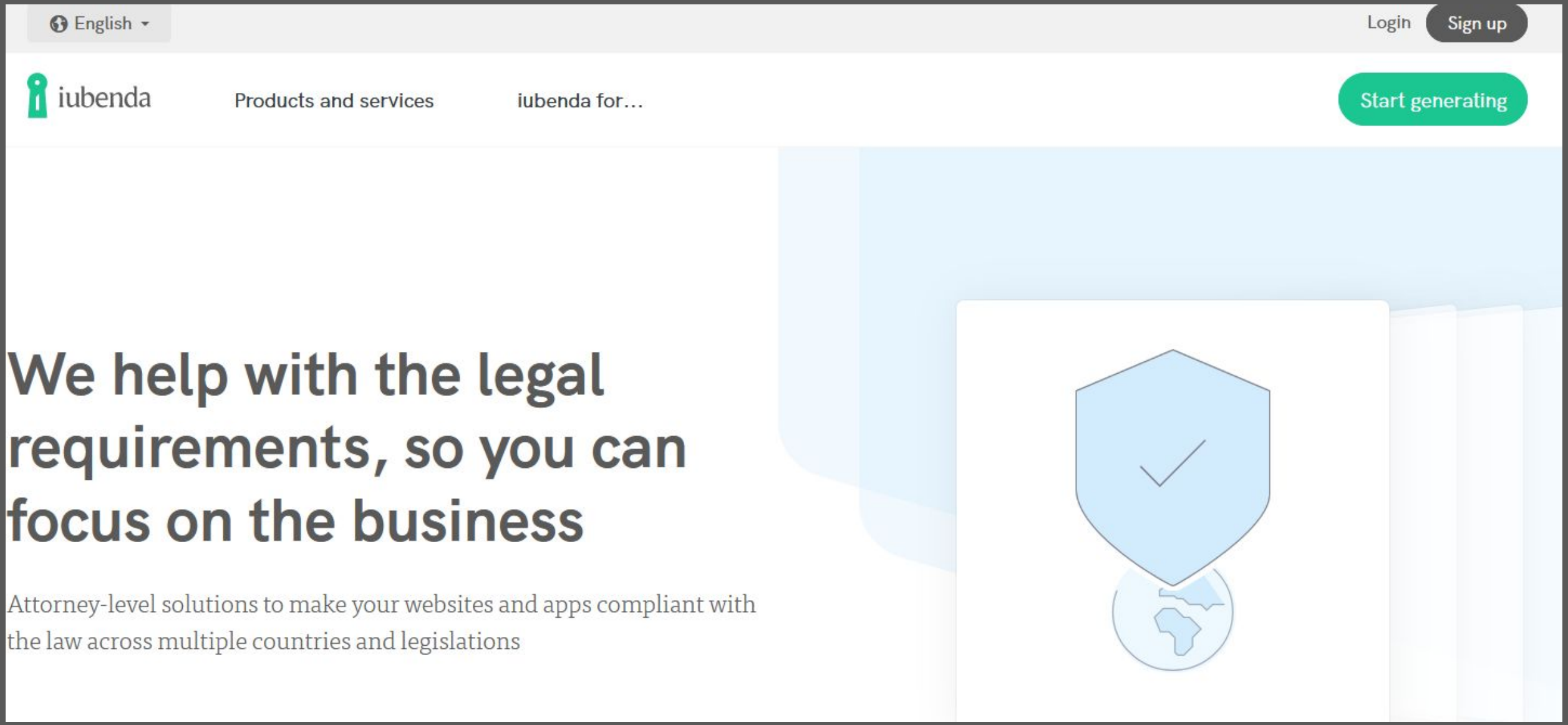
- DNS/HTTP(S)/SMTP(S)/LDAP Interaction
- CLI / Web / Burp / ZAP / Docker client
- AES encryption with zero logging
- Automatic ACME based Wildcard TLS w/ Auto Renewal
- DNS Entries for Cloud Metadata service
- Self-Hosted Interactsh Server
- Multiple domain support **(self-hosted)**

SPLUNK: ENDPOINT LOGS



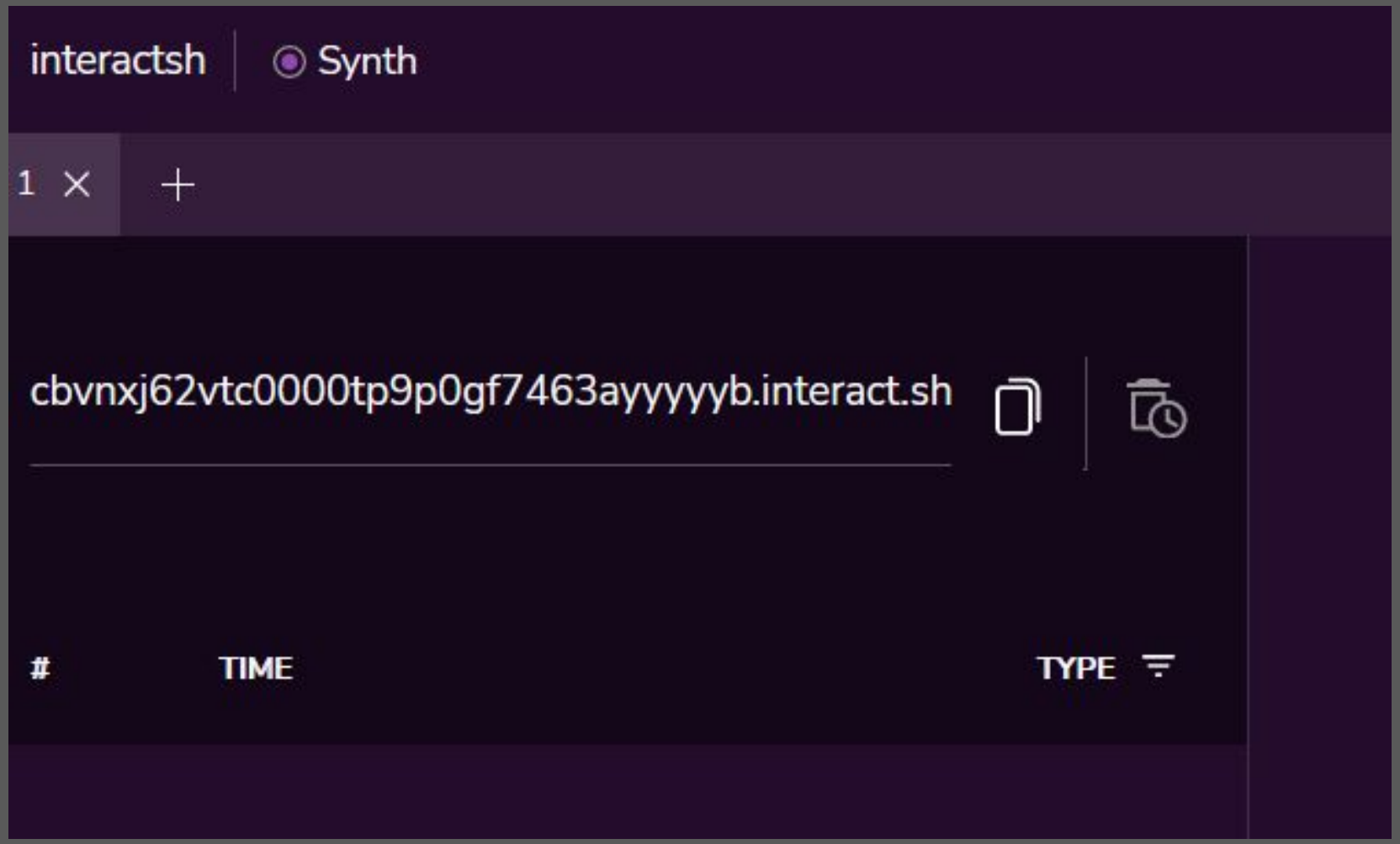
Source: https://app.interactsh.com/#/

SPLUNK: ENDPOINT LOGS



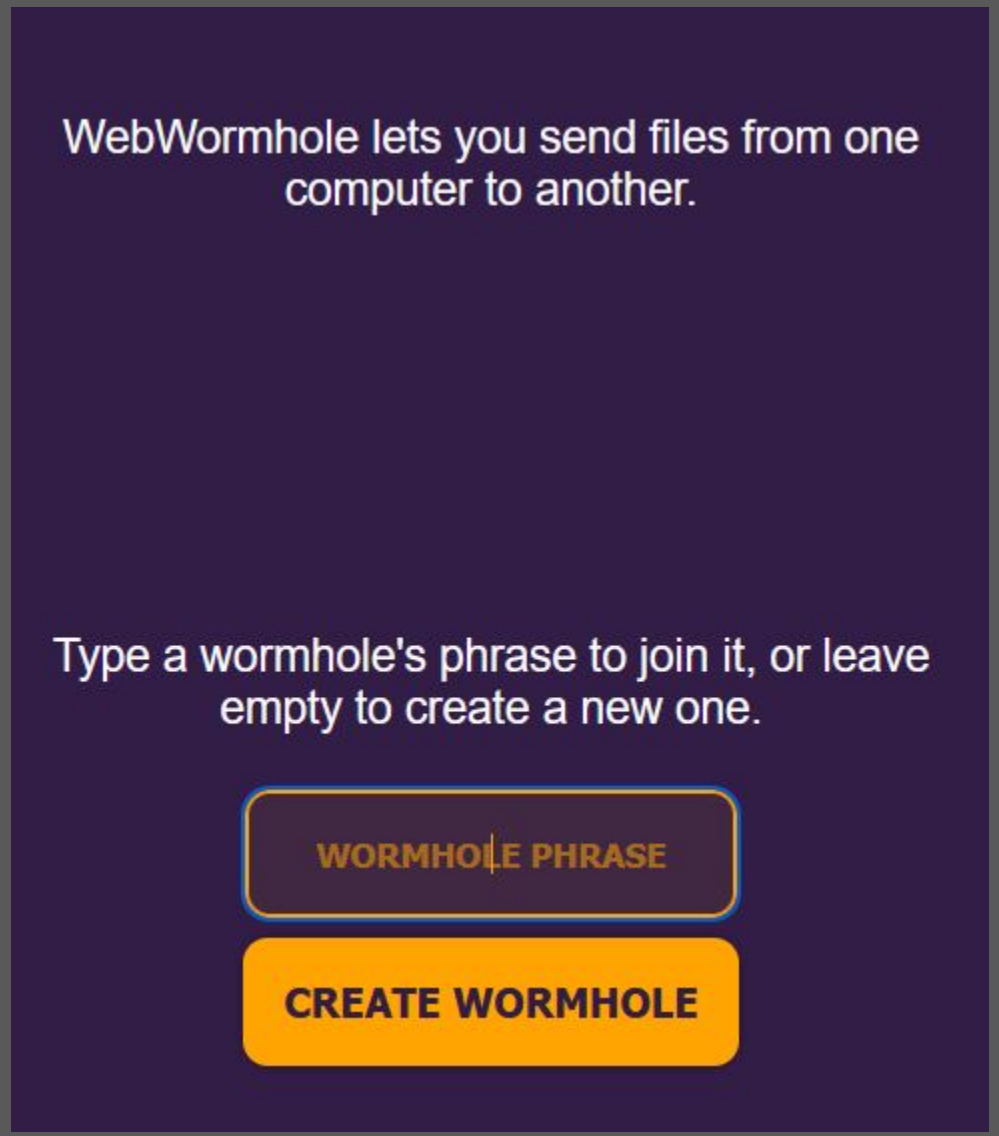
Source: https://www.iubenda.com/en/

SPLUNK: ENDPOINT LOGS



Source: https://app.interactsh.com/#/

SPLUNK: ENDPOINT LOGS



Source: https://webwormhole.io/

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
kerberos.ticket.cipher:* | groupby kerberos.request_type
kerberos.success kerberos.client kerberos.service
kerberos.ticket.renewable kerberos.ticket.forwardable
kerberos.ticket.valid.until source.ip destination.ip
```

SECURITY ONION: NETWORK LOGS

kerberos.request_type	kerberos.success	kerberos.client	kerberos.service	kerberos.ticket.renewable	kerberos.ticket.forwardable	kerberos.ticket.valid.until	source.ip
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst04.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/EC2AMAZ-LPQL4P6.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/EC2AMAZ-6IJTUBB.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/EC2AMAZ-6R2FQH5.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/files.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	LDAP/dc02.magnumtempus.financial/magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	krbtgt/MAGNUMTEMPUS.FINANCIAL	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	ProtectedStorage/dc02.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/dc.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/dc02.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/dc02.magnumtempus.financial/magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst03.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst05.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst06.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst07.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst08.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst10.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst11.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst12.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst13.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/wkst14.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	host/rdp01.magnumtempus.financial	true	true	2136422912	172.16.55.1
TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	ldap/dc.magnumtempus.financial/magnumtempus.financial	true	true	2136422912	172.16.55.1

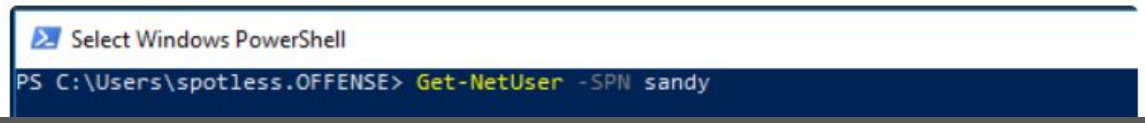
Kerberoasting: Requesting RC4 Encrypted TGS when AES is Enabled

It is possible to kerberoast a user account with SPN even if the account supports Kerberos AES encryption by requesting an RC4 ecnrypted (instead of AES) TGS which easier to crack.

Execution

First off, let's confirm we have at least one user with an SPN set:

```
attacker@victim
Get-NetUser -SPN sandy
```



Source: https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/kerberoasting-requesting-rc4-encrypted-tgs-when-aes-is-enabled

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

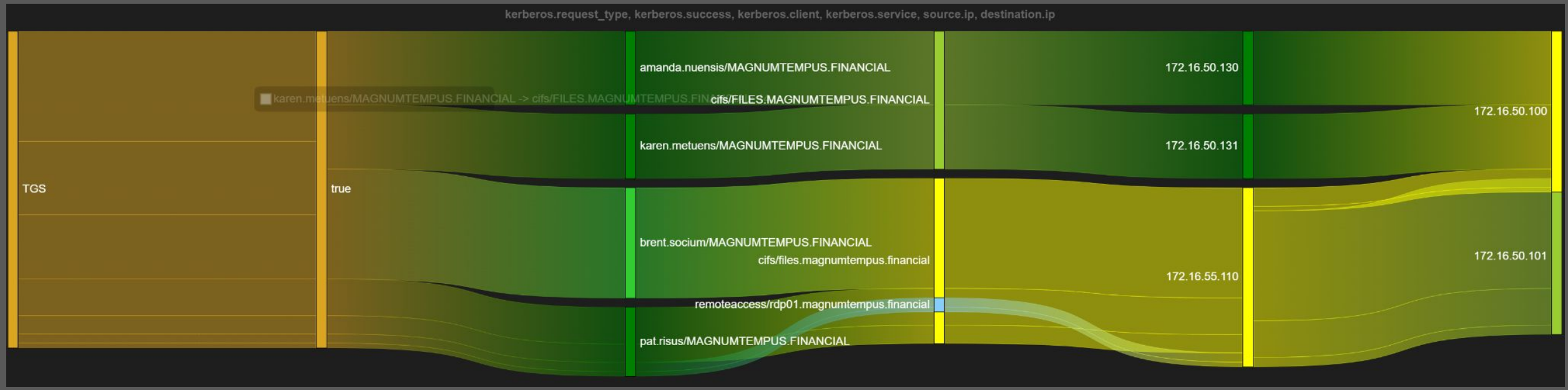
```
kerberos.ticket.cipher:”rc4*” | groupby @timestamp
kerberos.request type kerberos.success kerberos.client
kerberos.service kerberos.ticket.renewable kerberos.ticket.forwardable
kerberos.ticket.valid.until source.ip destination.ip
```

SECURITY ONION: NETWORK LOGS

Count	@timestamp	kerberos.request_type	kerberos.success	kerberos.client	kerberos.service	kerberos.ticket.renewable	kerberos.ticket.forwardable	kerberos.ticket.valid.until	source.ip	destination.ip
2	2022-02-19T20:21:38.224Z	TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/files.magnumtempus.financial	true	true	2136422912	172.16.55.110	172.16.50.100
1	2022-02-19T20:21:38.231Z	TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/files.magnumtempus.financial	true	true	2136422912	172.16.55.110	172.16.50.100
1	2022-02-19T20:21:38.238Z	TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	cifs/files.magnumtempus.financial	true	true	2136422912	172.16.55.110	172.16.50.100
1	2022-02-19T20:22:03.376Z	TGS	true	pat.risus/MAGNUMTEMPUS.FINANCIAL	remoteaccess/rdp01.magnumtempus.financial	true	true	2136422912	172.16.55.110	172.16.50.100

SECURITY ONION: NETWORK LOGS

```
kerberos.ticket.cipher:"rc4*" | groupby @timestamp kerberos.request_type
kerberos.success kerberos.client  kerberos.service source.ip
destination.ip
```



SECURITY ONION: NETWORK LOGS

rule.name
ET MALWARE Interactsh Control Panel (DNS)

network.data.decoded	L.....!c88nc6r2vtc00001pg0ggrrksdcyyyyyb.interact.sh.....

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
interact.sh | groupby @timestamp event.dataset rule.name* source.ip
destination.ip
```

SECURITY ONION: NETWORK LOGS

@timestamp	event.dataset	rule.name	source.ip	destination.ip
2022-02-19T20:43:07.850Z	alert	ET INFO Interactsh Domain in DNS Lookup (.interact .sh)	172.16.55.110	172.16.50.100
2022-02-19T20:43:07.850Z	alert	ET MALWARE Interactsh Control Panel (DNS)	172.16.55.110	172.16.50.100
2022-02-19T20:43:07.850Z	dns	*Missing	172.16.55.110	172.16.50.100
2022-02-19T20:41:30.958Z	alert	ET INFO Interactsh Domain in DNS Lookup (.interact .sh)	172.16.55.110	172.16.50.100
2022-02-19T20:41:30.958Z	dns	*Missing	172.16.55.110	172.16.50.100
2022-02-19T20:41:30.983Z	alert	ET INFO Interactsh Domain in DNS Lookup (.interact .sh)	172.16.55.110	172.16.50.100
2022-02-19T20:43:07.875Z	alert	ET INFO Interactsh Domain in DNS Lookup (.interact .sh)	172.16.55.110	172.16.50.100
2022-02-19T20:43:07.947Z	dns	*Missing	172.16.55.110	172.16.50.100
2022-02-19T20:41:30.975Z	dns	*Missing	172.16.55.110	172.16.50.100
2022-02-19T20:41:30.999Z	dns	*Missing	172.16.55.110	172.16.50.100
2022-02-19T20:41:31.000Z	dns	*Missing	172.16.55.110	172.16.50.100
2022-02-19T20:41:31.153Z	ssl	*Missing	172.16.55.110	46.101.25.250
2022-02-19T20:41:31.222Z	ssl	*Missing	172.16.55.110	46.101.25.250
2022-02-19T20:42:03.595Z	ssl	*Missing	172.16.55.110	46.101.25.250

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
interactsh.com | groupby @timestamp event.dataset rule.name* source.ip
destination.ip
```

SECURITY ONION: NETWORK LOGS

Count	@timestamp	event.dataset	rule.name	source.ip	destination.ip
4	2022-02-19T20:41:58.132Z	dns	*Missing	172.16.55.110	172.16.50.100
2	2022-02-19T20:41:57.995Z	ssl	*Missing	172.16.55.110	172.67.71.174
1	2022-02-19T20:41:57.995Z	dns	*Missing	172.16.55.110	172.16.50.100
1	2022-02-19T20:41:57.907Z	alert	ET INFO Interactsh Domain in DNS Lookup (.interactsh .com)	172.16.55.110	172.16.50.100
1	2022-02-19T20:41:57.907Z	dns	*Missing	172.16.55.110	172.16.50.100
2	2022-02-19T20:41:58.079Z	alert	ET INFO Interactsh Domain in DNS Lookup (.interactsh .com)	172.16.55.110	172.16.50.100
2	2022-02-19T20:41:58.105Z	alert	ET INFO Interactsh Domain in DNS Lookup (.interactsh .com)	172.16.55.110	172.16.50.100
1	2022-02-19T20:41:57.908Z	alert	ET INFO Interactsh Domain in DNS Lookup (.interactsh .com)	172.16.55.110	172.16.50.100

SECURITY ONION: NETWORK LOGS

```
"46.101.25.250" | groupby event.dataset
```

Count	event.dataset
25	alert
16	conn
6	dns
4	ssl
1	file
1	http

Dumping Processes

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:44:12 *to* 02/19/22 20:54:00

Splunk Search:

```
index=sysmon host.name="rdp01.magnumtempus.financial"
(event.code=1 OR event.code=22) _raw!="*Teams*"
| rename "dns.resolved_ip{}" as IP
| eval Info=mvappend('process.command_line','dns.question.name')
| mvexpand Info
| table _time index host.name event.code process.name Info IP
| sort _time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	process.name	Info	IP
2022-02-19 20:44:12	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	relay.webwormhole.io.	157.245.15.73
2022-02-19 20:46:57	sysmon	rdp01.magnumtempus.financial	1	Taskmgr.exe	"C:\Windows\System32\Taskmgr.exe" /2	
2022-02-19 20:46:57	sysmon	rdp01.magnumtempus.financial	1	Taskmgr.exe	"C:\Windows\System32\Taskmgr.exe" /2	
2022-02-19 20:47:59	sysmon	rdp01.magnumtempus.financial	1	tasklist.exe	"C:\Windows\system32\tasklist.exe" /M	
2022-02-19 20:48:09	sysmon	rdp01.magnumtempus.financial	1	tasklist.exe	"C:\Windows\system32\tasklist.exe" /M:rdpcorets.dll	
2022-02-19 20:48:48	sysmon	rdp01.magnumtempus.financial	1	rundll32.exe	"C:\windows\system32\rundll32.exe" C:\windows\System32\comsvcs.dll MiniDump 828 C:\dump full	
2022-02-19 20:51:08	sysmon	rdp01.magnumtempus.financial	22	powershell.exe	raw.githubusercontent.com	185.199.108.133 185.199.109.133 185.199.110.133 185.199.111.133
2022-02-19 20:51:39	sysmon	rdp01.magnumtempus.financial	1	WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	
2022-02-19 20:51:39	sysmon	rdp01.magnumtempus.financial	1	whoami.exe	"C:\Windows\system32\whoami.exe" /user	
2022-02-19 20:51:41	sysmon	rdp01.magnumtempus.financial	22	powershell.exe	RDP01	172.16.55.110

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	process.name	Info	IP
2022-02-19 20:52:15	sysmon	rdp01.magnumtempus.financial	1	whoami.exe	"C:\Windows\system32\whoami.exe" /user	
2022-02-19 20:52:22	sysmon	rdp01.magnumtempus.financial	1	cmd.exe	cmd.exe	
2022-02-19 20:53:02	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	play.google.com	172.217.0.174
2022-02-19 20:53:02	sysmon	rdp01.magnumtempus.financial	22	chrome.exe	live.sysinternals.com	52.154.170.73

Dumping SAM database & Mimikatz

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:51:08 *to* 02/19/22 21:01:08

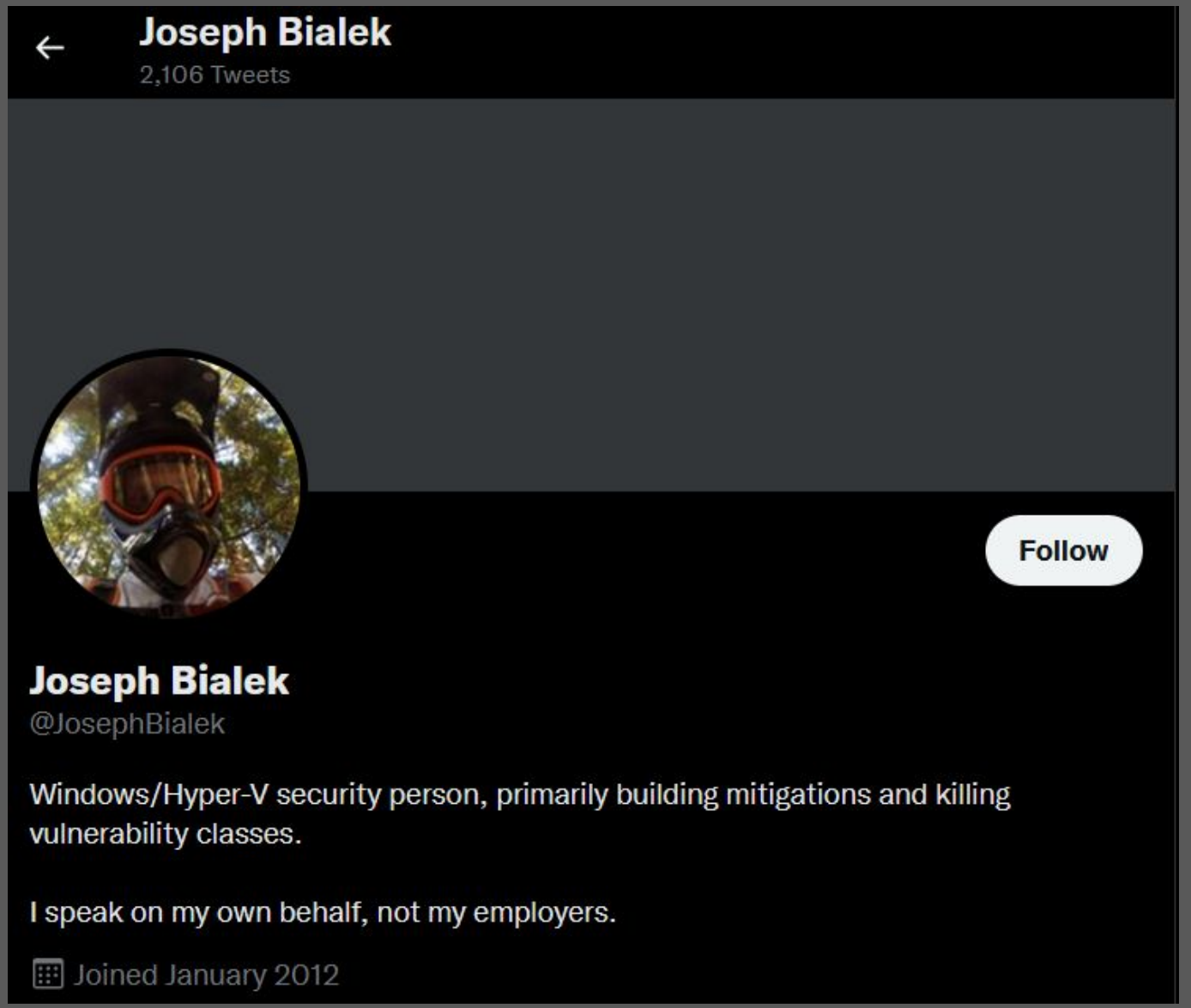
Splunk Search:

```
index=wineventlogs host.name="rdp01.magnumtempus.financial"
event.code=4104  raw="*Creating Scriptblock text (1 of *"
| rex field= raw "message\":\"(?<MessageExctracted>.+)"
| eval Message=MessageExctracted
| rex mode=sed field=Message "s/\\\n/*/g"
| makemv delim="*",Message
| rex mode=sed field=Message "s/\\\t/*/g"
| makemv delim="*",Message
| table  time index host.name event.code Message
| sort  time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	Message
2022-02-19 20:51:38.294	wineventlogs	rdp01.magnumtempus.financial	4104	Creating Scriptblock text (1 of 200): function Invoke-Mimikatz { <# .SYNOPSIS This script leverages Mimikatz 2.2.0 and Invoke-ReflectivePEInjection to reflectively load Mimikatz completely in memory. This allows you to do thin such as dump credentials without ever writing the mimikatz binary to disk. The script has a ComputerName parameter which allows it to be executed against multiple computers. This script should be able to dump credentials from any version of Windows through Windows 8.1 that has PowerShell v2 or higher installed. Function: Invoke-Mimikatz Author: Joe Bialek, Twitter: @JosephBialek Mimikatz Author: Benjamin DELPY `gentilkiwi`. Blog: http://blog.gentilkiwi.com. Email: benjamin@gentilkiwi.com. Twitter @gentilkiwi License: http://creativecommons.org/licenses/by/3.0/fr/

SPLUNK: ENDPOINT LOGS



Source: https://twitter.com/josephbialek

SPLUNK: ENDPOINT LOGS

SPLUNK: ENDPOINT LOGS

OS Credential Dumping: LSASS Memory

Other sub-techniques of OS Credential Dumping (8)

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- `procdump -ma lsass.exe lsass_dump`

ID: T1003.001

Sub-technique of: T1003

Tactic: Credential Access

Platforms: Windows

Contributors: Ed Williams, Trustwave, SpiderLabs; Edward Millington

Version: 1.1

Created: 11 February 2020

Last Modified: 12 May 2022

Version Permalink

Source: https://attack.mitre.org/techniques/T1003/001/

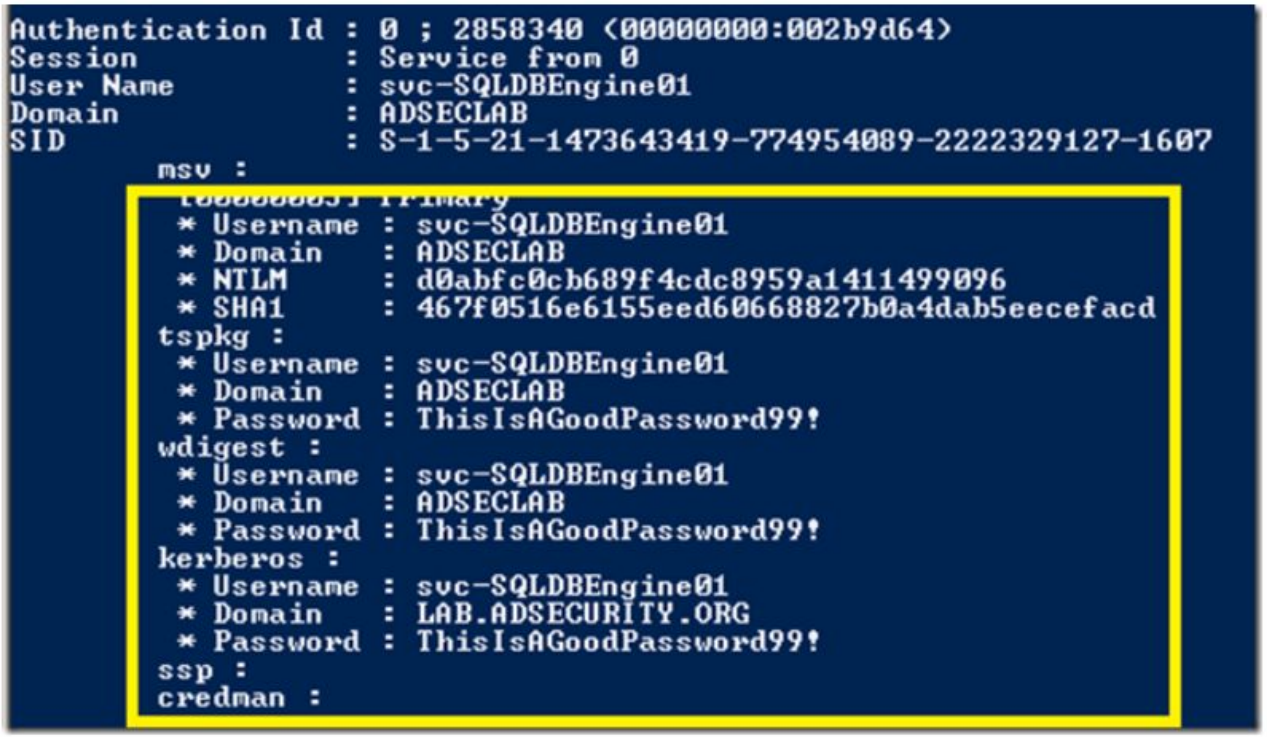
SPLUNK: ENDPOINT LOGS

SPLUNK: ENDPOINT LOGS

SPLUNK: ENDPOINT LOGS

Origin story of the Mimikatz password cracker is a parable about security, disclosure, cyberwar, and crime

CORY DOCTOROW / 11:45 PM THU NOV 9, 2017



Five years ago, Benjamin Delpy was working for an unspecified French government agency and teaching himself to program in C, and had discovered a vital flaw in the way that Windows protected its users' passwords.

SECURITY ONION: NETWORK LOGS

rule.name
ET POLICY Observed DNS Query to File Transfer Service Domain (transfer .sh)
ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in DNS Lookup)
ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in DNS Lookup)

network.data.decoded	.....j+./..u..+.ajA....o,...4]...G.. 6.....k..Xl..X.....2.G.t..y].. .. JJ.....+./.,.0...../.5.....transfer.sh..... .....#.....h2.http/1.1.....3.+.)..... ..u.&.....h-....1..h?...p#.q.-.....+...jj.....Di.....h2JJ.....

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
transfer.sh | groupby @timestamp event.dataset rule.name* source.ip
destination.ip
```

SECURITY ONION: NETWORK LOGS

@timestamp	event.dataset	rule.name	source.ip	destination.ip
2022-02-19T20:17:41.675Z	alert	ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in DNS Lookup)	172.16.55.110	172.16.50.100
2022-02-19T20:17:41.675Z	alert	ET POLICY Observed DNS Query to File Transfer Service Domain (transfer .sh)	172.16.55.110	172.16.50.100
2022-02-19T20:17:41.675Z	dns	*Missing	172.16.55.110	172.16.50.100
2022-02-19T20:17:41.790Z	ssl	*Missing	172.16.55.110	144.76.136.153
2022-02-19T20:17:41.823Z	ssl	*Missing	172.16.55.110	144.76.136.153
2022-02-19T20:17:41.890Z	alert	ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in TLS SNI)	172.16.55.110	144.76.136.153
2022-02-19T20:17:41.911Z	alert	ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in TLS SNI)	172.16.55.110	144.76.136.153
2022-02-19T20:47:33.877Z	ssl	*Missing	172.16.55.110	144.76.136.153
2022-02-19T20:47:33.975Z	alert	ET INFO Commonly Abused File Sharing Site Domain Observed (transfer .sh in TLS SNI)	172.16.55.110	144.76.136.153

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
144.76.136.153 | groupby event.dataset
```

SECURITY ONION: NETWORK LOGS

Count	event.dataset
6	alert
6	conn
6	dns
6	ssl

Adding Users

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 20:51:38 *to* 02/19/22 21:51:00

Splunk Search:

```
index=sysmon host.name="rdp01.magnumtempus.financial"
event.code=1 process.command_line!="*teams*"
| rename process.command_line as CommandLine
| table  time index host.name event.code user.name CommandLine
| sort  _time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	user.name	CommandLine
2022-02-19 20:51:39	sysmon	rdp01.magnumtempus.financial	1	NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
2022-02-19 20:51:39	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 20:52:15	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 20:52:22	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	cmd.exe
2022-02-19 20:55:03	sysmon	rdp01.magnumtempus.financial	1	pat.risus	C:\Windows\System32\rundll32.exe shell32.dll,SHCreateLocalServerRunDll {c82192ee-6cb5-4bc0-9ef0-fb818773790a} -Embedding
2022-02-19 20:59:36	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\computers.txt net user combosecurity B4bymeta! /ADD
2022-02-19 21:02:11	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\pat.risus\Desktop\computers.txt
2022-02-19 21:02:28	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\brent.socium\computers.txt
2022-02-19 21:03:11	sysmon	rdp01.magnumtempus.financial	1	NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
2022-02-19 21:03:11	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:03:19	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	cmd.exe
2022-02-19 21:03:23	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:03:29	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	cmd.exe
2022-02-19 21:03:32	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:03:41	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	cmd.exe
2022-02-19 21:03:50	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\brent.socium\computers.txt
2022-02-19 21:04:27	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\brent.socium\1.txt
2022-02-19 21:04:49	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\brent.socium\2.txt
2022-02-19 21:05:13	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\brent.socium\3.txt
2022-02-19 21:12:32	sysmon	rdp01.magnumtempus.financial	1	NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	user.name	CommandLine
2022-02-19 21:12:32	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:12:41	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	cmd.exe
2022-02-19 21:13:01	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\pat.risus\Desktop\computers.txt net localgroup administrators combosecurity /ADD
2022-02-19 21:14:30	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\computers.txt net localgroup administrators combosecurity /ADD
2022-02-19 21:15:09	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\computers.txt net localgroup administrators combosecurity /ADD
2022-02-19 21:15:30	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\computers.txt localgroup "Remote Desktop Users" combosecurity /ADD
2022-02-19 21:17:17	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\1.txt net user andy B1rdD0g! /ADD
2022-02-19 21:17:30	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\2.txt net user hass C4rb4n4k! /ADD
2022-02-19 21:17:37	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\3.txt net user jimbo Dr1ftp1n! /ADD
2022-02-19 21:17:49	sysmon	rdp01.magnumtempus.financial	1	NETWORK SERVICE	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
2022-02-19 21:17:49	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:17:57	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	cmd.exe
2022-02-19 21:18:01	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:18:12	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	cmd.exe
2022-02-19 21:18:30	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\whoami.exe" /user
2022-02-19 21:18:39	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	cmd.exe
2022-02-19 21:19:04	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\3.txt net localgroup administrators jimbo /ADD
2022-02-19 21:19:13	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\3.txt net localgroup "Remote Desktop Users" jimbo /ADD
2022-02-19 21:19:22	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\2.txt net localgroup "Remote Desktop Users" hass /ADD
2022-02-19 21:19:48	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\2.txt net localgroup administrators hass /ADD

SPLUNK: ENDPOINT LOGS

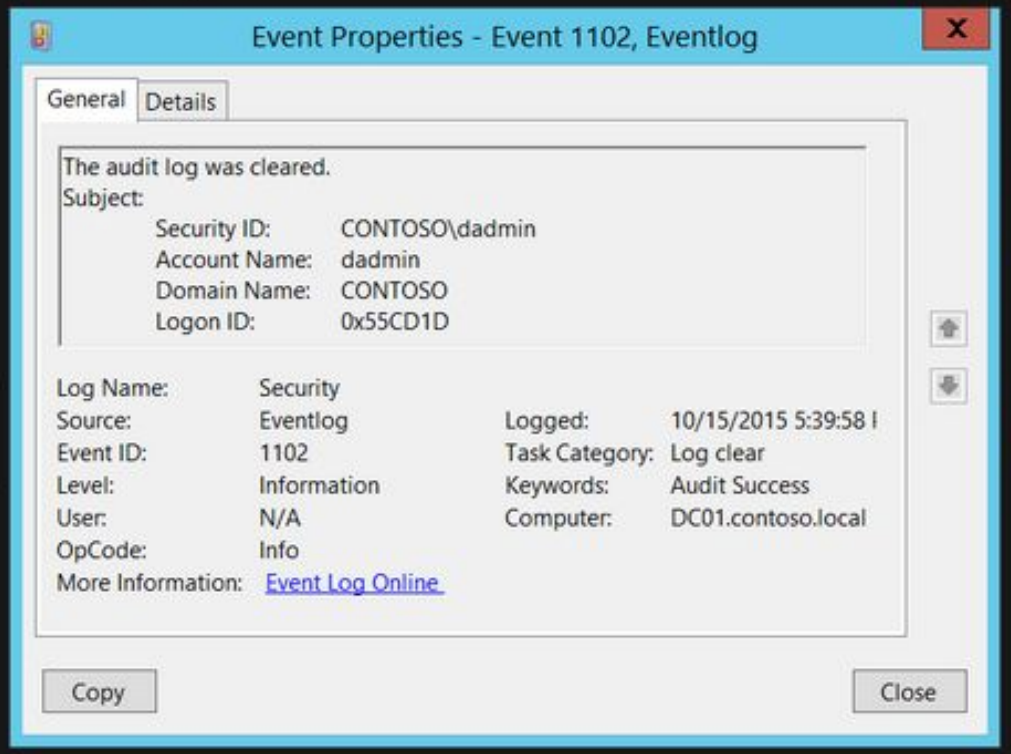
_time	index	host.name	event.code	user.name	CommandLine
2022-02-19 21:21:27	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\1.txt net localgroup administrators andy /ADD
2022-02-19 21:21:35	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\1.txt net localgroup "Remote Desktop Users" andy /ADD
2022-02-19 21:26:46	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\computers.txt powershell.exe "& {Clear-EventLog -Log Application,System,Security}"
2022-02-19 21:27:28	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\brent.socium\computers.txt
2022-02-19 21:27:55	sysmon	rdp01.magnumtempus.financial	1	pat.risus	"C:\Windows\system32\NOTEPAD.EXE" C:\Users\brent.socium\Desktop\computers.txt
2022-02-19 21:28:19	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\computers.txt "& {Clear-Eventlog -Log Application,System,Security}"
2022-02-19 21:30:05	sysmon	rdp01.magnumtempus.financial	1	SYSTEM	.\PsExec64.exe @C:\Users\brent.socium\Desktop\computers.txt powershell.exe -command "& {Clear-Eventlog -Log Application,System,Security}"

Wiping Event Logs

SPLUNK: ENDPOINT LOGS

1102(S): The audit log was cleared.

Article • 12/14/2021 • 2 minutes to read • 9 contributors



Subcategory: Other Events

Event Description:

This event generates every time Windows Security audit log was cleared.

Note For recommendations, see Security Monitoring Recommendations for this event.

Source: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-1102

SPLUNK: ENDPOINT LOGS

Set date/time between 02/19/22 21:26:46 *to* 02/19/22 21:32:00

Splunk Search:

```
index=wineventlogs host.name="rdp01.magnumtempus.financial"
event.code=1102
| table  time index host.name event.code message
| sort _time
```

SPLUNK: ENDPOINT LOGS

_time	index	host.name	event.code	message
2022-02-19 21:30:44.758	wineventlogs	rdp01.magnumtempus.financial	1102	The audit log was cleared. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Domain Name: NT AUTHORITY Logon ID: 0x3E7

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
event.dataset:file | groupby file.mime_type*
```

SECURITY ONION: NETWORK LOGS

Count	file.mime_type
1,683	application/x-x509-ca-cert
823	application/x-x509-user-cert
174	*Missing
157	text/ini
106	text/plain
74	application/xml
72	application/ocsp-response
61	application/x-dosexec
40	application/chrome-ext
21	text/html
16	application/zip
12	application/vnd.openxmlformats-officedocument.wordprocessingml.document
8	image/jpeg
4	application/msword
4	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
4	text/rtf
2	application/chrome-ext-upd
2	application/pdf
2	application/vnd.openxmlformats-officedocument.presentationml.presentation
2	image/png
1	application/vnd.ms-pol

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
event.dataset:file AND file.mime_type:"application/x-dosexec" |
groupby file.name*
```

SECURITY ONION: NETWORK LOGS

Count	file.name
61	PSEXESVC.exe

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

```
event.dataset:file AND file.name:"PSEXESVC.exe" | groupby source.ip destination.ip
```

SECURITY ONION: NETWORK LOGS

Count	source.ip	destination.ip
9	172.16.55.110	172.16.50.100
6	172.16.55.110	172.16.50.133
6	172.16.55.110	172.16.50.140
5	172.16.55.110	172.16.50.130
5	172.16.55.110	172.16.50.131
5	172.16.55.110	172.16.50.132
5	172.16.55.110	172.16.50.134
5	172.16.55.110	172.16.50.138
4	172.16.55.110	172.16.50.101
4	172.16.55.110	172.16.50.135
4	172.16.55.110	172.16.50.137
3	172.16.55.110	172.16.50.136
3	172.16.55.110	172.16.50.139
3	172.16.55.110	172.16.50.141
3	172.16.55.110	172.16.50.142
3	172.16.55.110	172.16.50.143
3	172.16.55.110	172.16.50.144

SECURITY ONION: NETWORK LOGS

Set date/time between 02/19/22 12:00 AM *to* 02/19/22 11:59 PM

Security Onion Search:

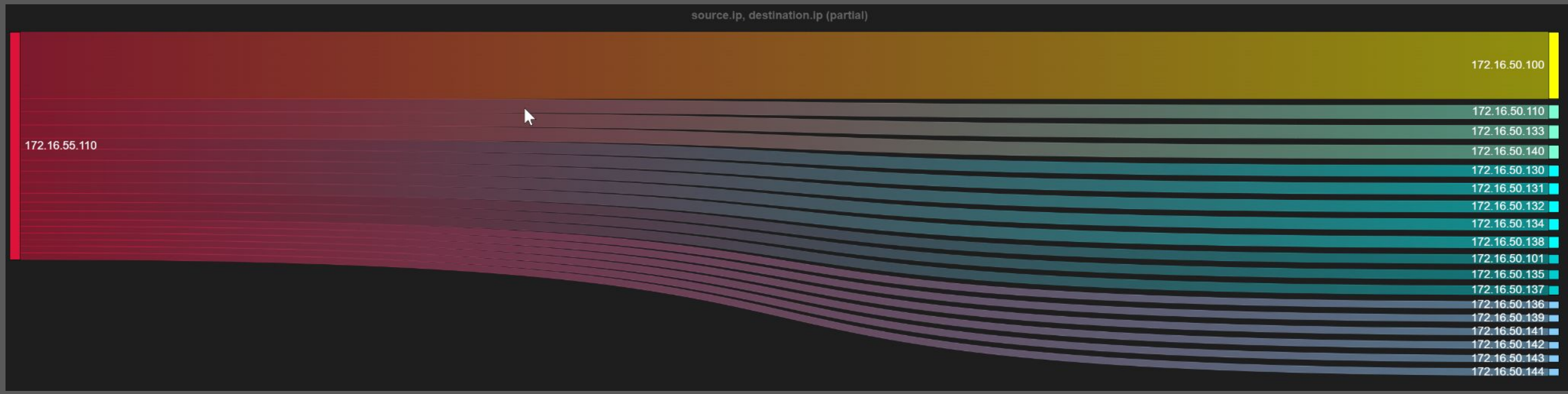
```
event.dataset:file AND file.name:"PSEXESVC.exe" | groupby @timestamp
source.ip destination.ip
```

SECURITY ONION: NETWORK LOGS

Count	@timestamp	source.ip	destination.ip
2	2022-02-19T20:59:36.096Z	172.16.55.110	172.16.50.100
1	2022-02-19T20:59:57.615Z	172.16.55.110	172.16.50.101
1	2022-02-19T21:00:40.337Z	172.16.55.110	172.16.50.130
1	2022-02-19T21:01:17.115Z	172.16.55.110	172.16.50.131
1	2022-02-19T21:01:48.125Z	172.16.55.110	172.16.50.132
1	2022-02-19T21:02:10.101Z	172.16.55.110	172.16.50.133
1	2022-02-19T21:02:49.154Z	172.16.55.110	172.16.50.134
1	2022-02-19T21:03:29.753Z	172.16.55.110	172.16.50.135
1	2022-02-19T21:05:50.244Z	172.16.55.110	172.16.50.138
1	2022-02-19T21:07:21.749Z	172.16.55.110	172.16.50.140
1	2022-02-19T21:08:03.637Z	172.16.55.110	172.16.50.141
1	2022-02-19T21:08:56.454Z	172.16.55.110	172.16.50.142
1	2022-02-19T21:09:42.857Z	172.16.55.110	172.16.50.143
1	2022-02-19T21:15:07.149Z	172.16.55.110	172.16.50.100
1	2022-02-19T21:15:07.166Z	172.16.55.110	172.16.50.100
1	2022-02-19T21:15:28.469Z	172.16.55.110	172.16.50.101
1	2022-02-19T21:15:28.479Z	172.16.55.110	172.16.50.101
1	2022-02-19T21:16:11.236Z	172.16.55.110	172.16.50.130
1	2022-02-19T21:16:32.161Z	172.16.55.110	172.16.50.130
1	2022-02-19T21:16:32.647Z	172.16.55.110	172.16.50.131
1	2022-02-19T21:16:53.493Z	172.16.55.110	172.16.50.131
1	2022-02-19T21:16:54.198Z	172.16.55.110	172.16.50.132
1	2022-02-19T21:17:14.745Z	172.16.55.110	172.16.50.132
1	2022-02-19T21:17:15.860Z	172.16.55.110	172.16.50.133
1	2022-02-19T21:17:34.714Z	172.16.55.110	172.16.50.140

SECURITY ONION: NETWORK LOGS

```
event.dataset:file AND file.name:"PSEXESVC.exe" | groupby -sankey
@timestamp source.ip destination.ip
```



SECURITY ONION: NETWORK LOGS

Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name	rule.category
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.200 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.198 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY PsExec service created	A suspicious filename was detected
2022-02-19 21:16:54.180 +00:00	172.16.55.110	51281	172.16.50.131	445	ET POLICY PsExec service created	A suspicious filename was detected

SECURITY ONION: NETWORK LOGS

Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name
2022-02-19 21:16:54.198 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY SMB Executable File Transfer
2022-02-19 21:16:54.198 +00:00	172.16.55.110	51285	172.16.50.132	445	ET POLICY SMB Executable File Transfer
2022-02-19 21:16:53.493 +00:00	172.16.55.110	51279	172.16.50.131	445	ET POLICY SMB Executable File Transfer
2022-02-19 21:16:53.493 +00:00	172.16.55.110	51279	172.16.50.131	445	ET POLICY SMB Executable File Transfer
2022-02-19 21:16:53.188 +00:00	172.16.55.110	51266	172.16.50.130	445	ET POLICY SMB Executable File Transfer
2022-02-19 21:16:53.188 +00:00	172.16.55.110	51266	172.16.50.130	445	ET POLICY SMB Executable File Transfer

SECURITY ONION: NETWORK LOGS

```
event.dataset:alert | groupby rule.name
```

Count	rule.name
174	ET POLICY PsExec service created
49	ET POLICY SMB2 NT Create AndX Request For an Executable File
33	ET POLICY SMB Executable File Transfer
11	ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
10	ET POLICY DNS Update From External net

Summary of Findings

(Splunk)	RDP login from 3.129.164.140
(Security Onion)	Confirmation of RDP login from 3.129.164.140
(Splunk)	Evidence of Active Directory enumeration using Invoke-Bloodhound
(Splunk)	Evidence of possible data exfiltration using "file.pizza"
(Splunk)	Evidence of possible port scanning using “Invoke-Portscan”
(Security Onion)	Confirmation of port scanning
(Splunk)	Evidence of “PowerView” PowerShell script used to enumerate AD
(Splunk)	Evidence of Kerberoasting
(Security Onion)	Confirmation of Kerberoasting
(Splunk)	Evidence of out of band Data Extraction using “interact.sh”
(Security Onion)	Confirmation of out of band Data Extraction using “interact.sh”
(Splunk)	Evidence of dumping processes
(Security Onion)	Confirmation of dumping processes
(Splunk)	Evidence of dumping SAM database & Mimikatz
(Splunk)	Evidence of attacker creating user accounts
(Splunk)	Evidence of attacker wiping the Windows Event logs
(Security Onion)	Confirmation of attacker wiping the Windows Event logs

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:

@_sandw1ch

Obsidian Red Team!

Obsidian Engineering Team!

Project Obsidian

THANK YOU!

join the conversation

https://discord.blueteamvillage.org