ResponderCon

Have Fun with It!: Tracking Ransomware Operator Lateral Movement and Recovering Deleted Files the *Easy Way*!

Ryan Chapman | **@rj_chap**

I'm a HACKER ABOUT ME

CactusCon

Ryan Chapman | @rj_chap

- Principal IR Consultant @ BlackBerry
- Author of SANS **FOR528: Ransomware for Incident Responders**
- **CactusCon** Sponsor/Community Liaison (former Lead)
- PluralSight author
- Retro gaming enthusiast

ResponderCon

Our Focus

- **Quick-and-easy, FREE** tools
- Tools that enable **at-a-glance analysis**
- Per-host analysis == easy
- **Boots on the ground?** Perfect!
- Especially applicable to Law Enforcement (LE)!
  - We are often asked about LE resources
  - These work great!

LOGONTRACER

Eric Zimmerman's
TOOLS


Tracking Lateral
Movement

Tracking Lateral Movement

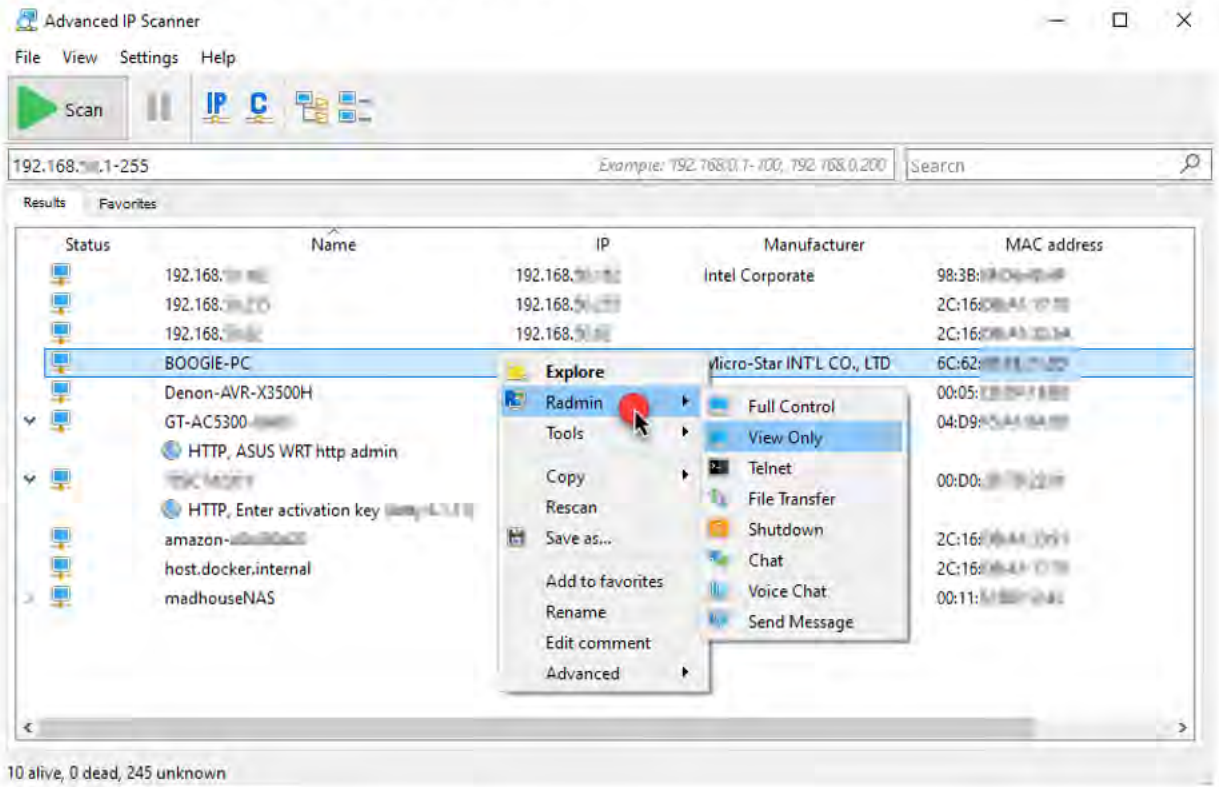
- Tracking the adversary through the network
- Common lateral movement methods:
  - SMB
  - RDP
  - BITS
  - WinRM
  - WMI
- SMB is the most popular – e.g., PsExec & related methods
  - Want to learn *exactly* how PsExec works? See for528.com/psexec-lateral
- For an amazing LM tracking sheet, see for528.com/lateral

Scanning… Scanning… Scanning…

- To move laterally, the TA must know where to go
- Commercial, free, and FOSS scanners used often

[from FOR528 Section 2]

- Ransomware actors tend to prefer these scanners:
  - Advanced IP Scanner
  - Advanced Port Scanner
  - Angry IP Scanner
  - Cobalt Strike (built-in scanning)
  - KPort Scanner
  - Network Port Scanner
  - nmap (good old nmap!)
  - Qfinder Pro



LogonTracer to the Rescue!

- Tool to visualize lateral movement
- From JPCERT Coordination Center (JPCERT/CC)
- See the LogonTracer repo: for528.com/ltracer
- **IMPORTANT:**
  - Does not cover "***all***" logon/ authentication events
  - Event IDs included →

LOGONTRACER

Concept

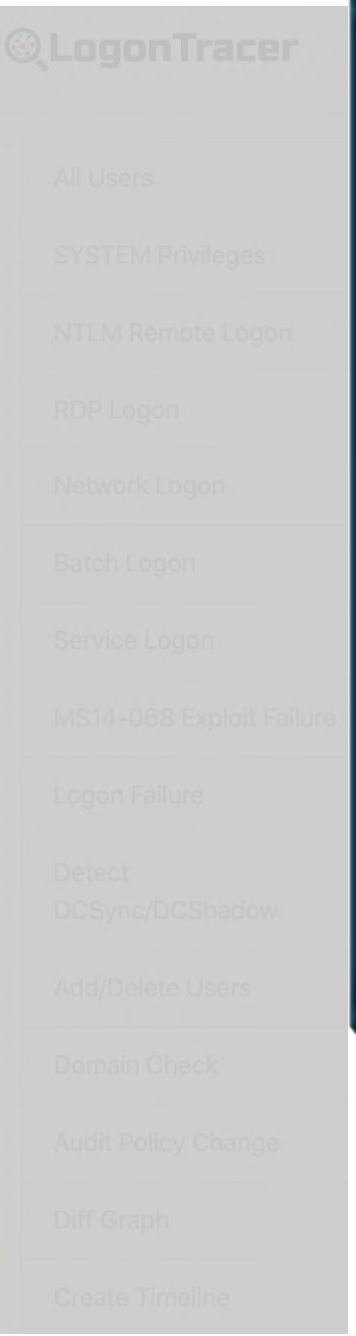
LogonTracer is a tool to investigate malicious logon by visualizing and analyzing Windows Active Directory event logs. This tool associates a host name (or an IP address) and account name found in logon-related events and displays it as a graph. This way, it is possible to see in which account login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

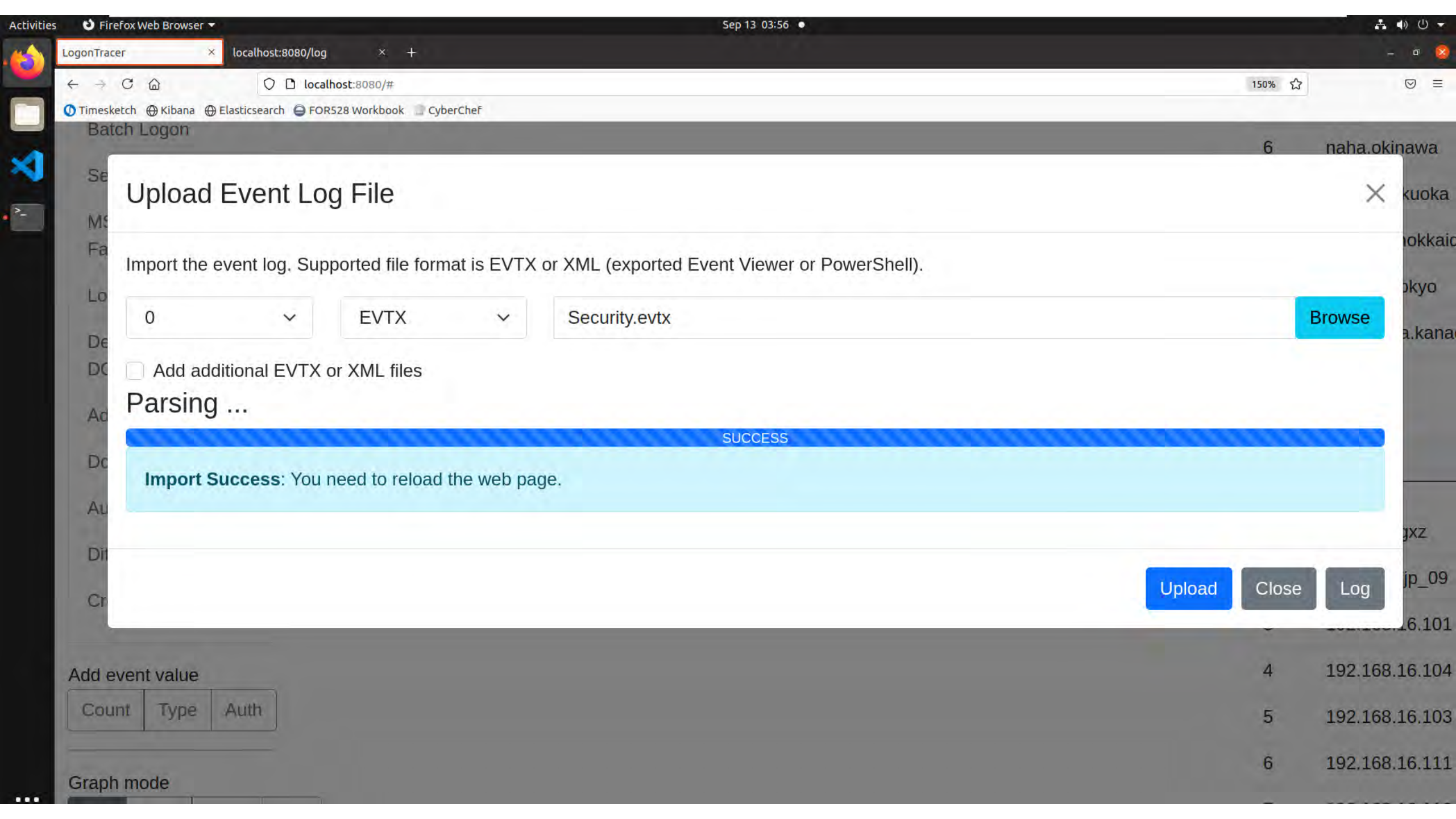
- **4624**: Successful logon
- **4625**: Logon failure
- **4768**: Kerberos Authentication (TGT Request)
- **4769**: Kerberos Service Ticket (ST Request)
- **4776**: NTLM Authentication
- **4672**: Assign special privileges

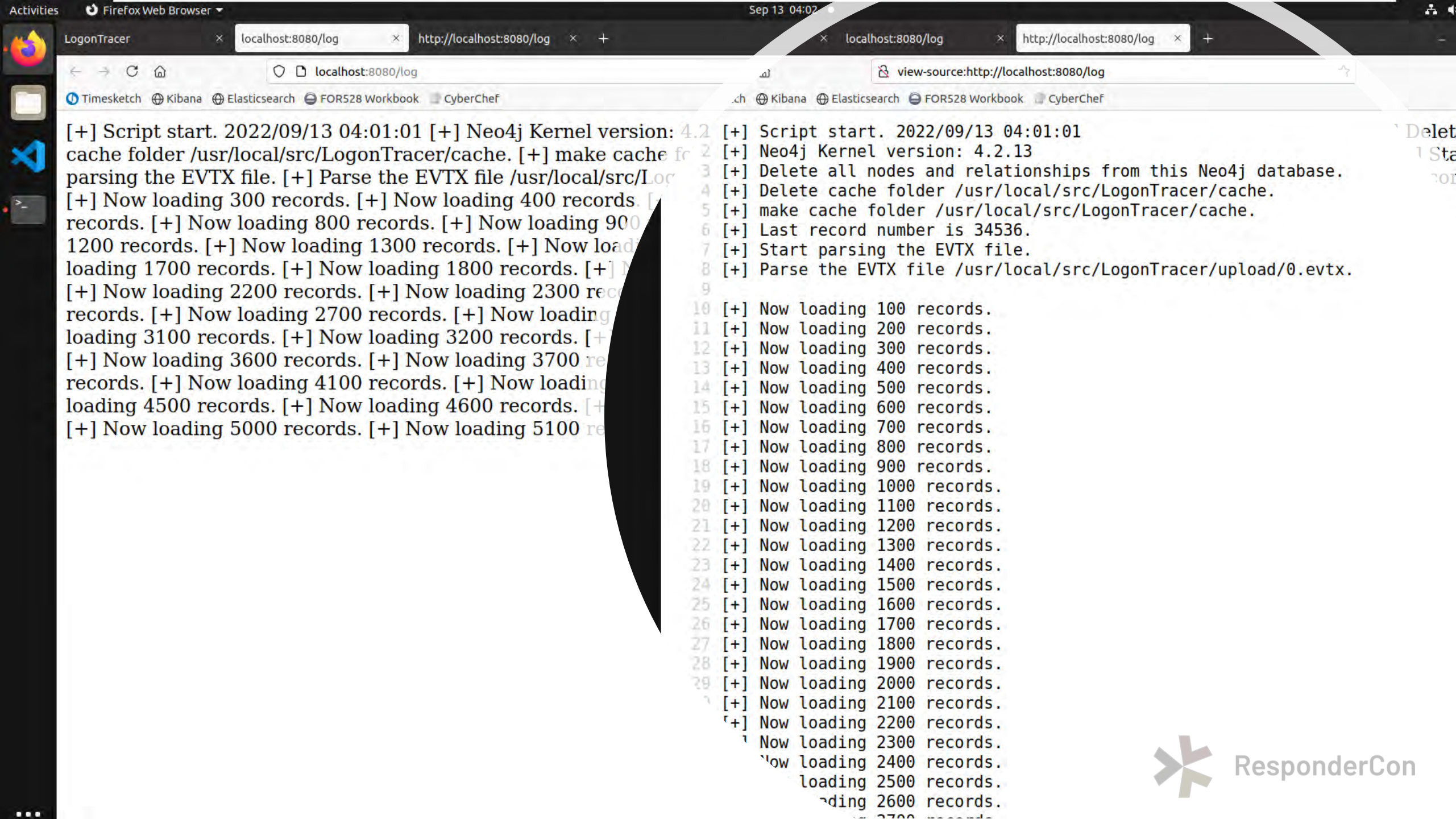
Installing LogonTracer

- Linux / macOS install
  - for528.com/ltracer-install
- Docker install
  - for528.com/ltracer-docker
  - E.g., Docker installed in FOR528 SIFT VM
  - `$ docker run --detach --publish=7474:7474 --publish=7687:7687 --publish=8080:8080 -e LTHOSTNAME=127.0.0.1 jpcertcc/docker-logontracer`

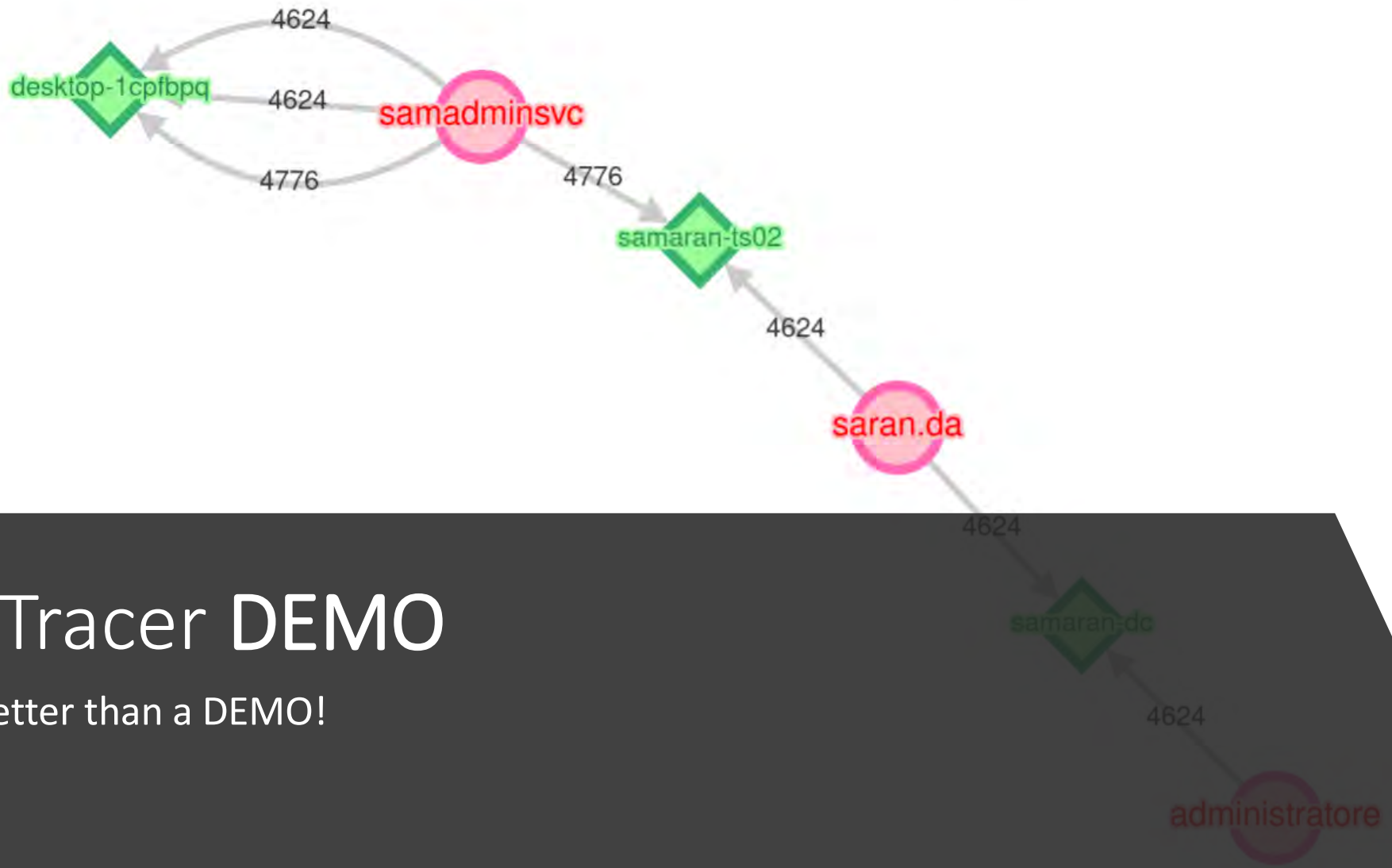
```
sansforensics@siftworkstation: ~
$ sudo docker run --detach --publish=7474:7474 --publish=7687:7687 --publish=8080:8080
 -e LTHOSTNAME=127.0.0.1 jpcertcc/docker-logontracer
97c6c5d630ecbcdf79b217159c37fdcfffcac757f4838d159fce596fd42d745f
```




Activities
Firefox Web Browser
Sep 13 03:56
LogonTracer
localhost:8080/log
localhost:8080/#
150%
Timesketch
Kibana
Elasticsearch
FOR528 Workbook
CyberChef
Batch Logon
Upload Event Log File
Import the event log. Supported file format is EVTX or XML (exported Event Viewer or PowerShell).
0
EVTX
Security.evtx
Browse
Add additional EVTX or XML files
Parsing ...
SUCCESS
Import Success: You need to reload the web page.
Upload
Close
Log
Add event value
Count
Type
Auth
Graph mode
6 naha.okinawa
4 192.168.16.104
5 192.168.16.103
6 192.168.16.111


Activities
Firefox Web Browser
Sep 13 04:02
LogonTracer
localhost:8080/log
http://localhost:8080/log
localhost:8080/log
http://localhost:8080/log
localhost:8080/log
view-source:http://localhost:8080/log
Timesketch
Kibana
Elasticsearch
FOR528 Workbook
CyberChef
Kibana
Elasticsearch
FOR528 Workbook
CyberChef
[+] Script start. 2022/09/13 04:01:01 [+] Neo4j Kernel version: 4.2
cache folder /usr/local/src/LogonTracer/cache. [+] make cache
parsing the EVTX file. [+] Parse the EVTX file /usr/local/src/
[+] Now loading 300 records. [+] Now loading 400 records.
records. [+] Now loading 800 records. [+] Now loading 90
1200 records. [+] Now loading 1300 records. [+] Now loa
loading 1700 records. [+] Now loading 1800 records. [+]
[+] Now loading 2200 records. [+] Now loading 2300
records. [+] Now loading 2700 records. [+] Now loadi
loading 3100 records. [+] Now loading 3200 records. [
[+] Now loading 3600 records. [+] Now loading 3700
records. [+] Now loading 4100 records. [+] Now loadi
loading 4500 records. [+] Now loading 4600 records.
[+] Now loading 5000 records. [+] Now loading 5100
[+] Script start. 2022/09/13 04:01:01
[+] Neo4j Kernel version: 4.2.13
[+] Delete all nodes and relationships from this Neo4j database.
[+] Delete cache folder /usr/local/src/LogonTracer/cache.
[+] make cache folder /usr/local/src/LogonTracer/cache.
[+] Last record number is 34536.
[+] Start parsing the EVTX file.
[+] Parse the EVTX file /usr/local/src/LogonTracer/upload/0.evtx.
[+] Now loading 100 records.
[+] Now loading 200 records.
[+] Now loading 300 records.
[+] Now loading 400 records.
[+] Now loading 500 records.
[+] Now loading 600 records.
[+] Now loading 700 records.
[+] Now loading 800 records.
[+] Now loading 900 records.
[+] Now loading 1000 records.
[+] Now loading 1100 records.
[+] Now loading 1200 records.
[+] Now loading 1300 records.
[+] Now loading 1400 records.
[+] Now loading 1500 records.
[+] Now loading 1600 records.
[+] Now loading 1700 records.
[+] Now loading 1800 records.
[+] Now loading 1900 records.
[+] Now loading 2000 records.
[+] Now loading 2100 records.
[+] Now loading 2200 records.
Now loading 2300 records.
loading 2400 records.
loading 2500 records.
ding 2600 records.
ResponderCon

onTracer Username farts + - Filter search search path Export Dark Mode



Rank	User
1	administrato
2	test
3	admin
4	gebruiker
5	canon
6	copier
7	contabilidac
8	george
9	it
10	jack

Back Next

Rank	Host
1	windows10
2	181.214.206.1
3	85.234.37.182
4	freerdp
5	windows2019
6	samaran-dc

LogonTracer DEMO

- Nothin' better than a DEMO!

Recovering MFT-Resident Files

MFT-Resident Files

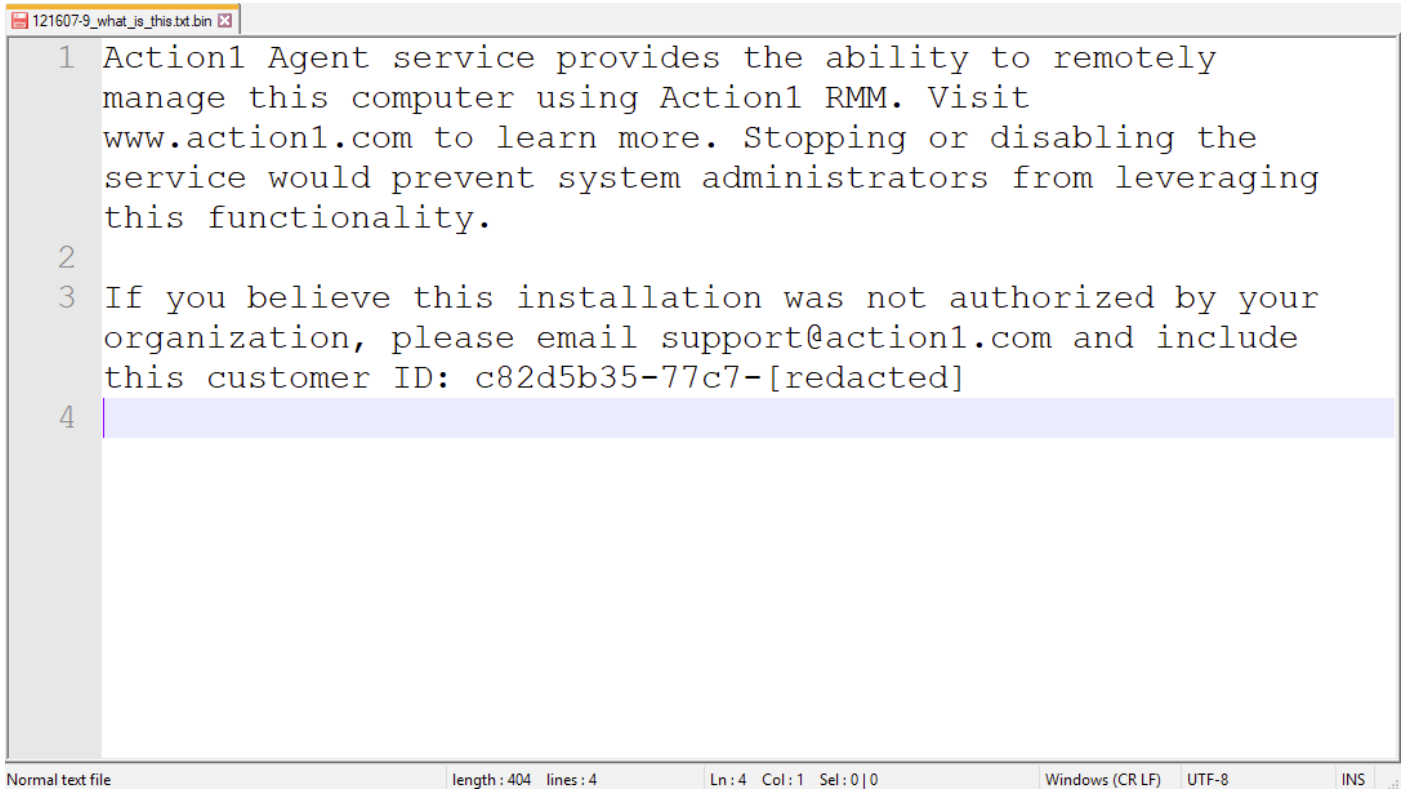
- Master File Table (MFT) overview
- Small files such as text and various script files may be “resident”
  - Triage collections often pull the $MFT file
  - With just this $MFT file, you may be able to obtain files
  - Even if *deleted*, you may be able to recover files from the $MFT itself (win!)
- MFT records are 1KB
  - 1KB == 1024 bytes
- If a file’s size, including NTFS metadata, is <1,024 bytes:
  - The file may reside within the $MFT file itself
- Maximum MFT-resident file sizes vary
  - Max size commonly accepted to be ~900 bytes
  - 1,000-byte files with *very* little NTFS metadata *could* be resident
- To learn more, see MS’ docs here: for528.com/resident

MFTEcmd to the Rescue!

- Eric Zimmerman's $MFT | $J | $LogFile | $Boot | $SDS parser
  - See for528.com/mftecmd
  - Eric's intro to his tool here: for528.com/mftecmd-intro
- "ZimmermanTools" are the go-to for many DFIR analysts
  - See https://ericzimmerman.github.io/
- A fun "small world" story:
  - Eric was in our FOR528 alpha chat
  - During class, a student noted how useful it would be if MFTEcmd could dump *all* resident files in one fell swoop
  - Within an hour, MFTEcmd was updated! (Thanks again Eric!!)

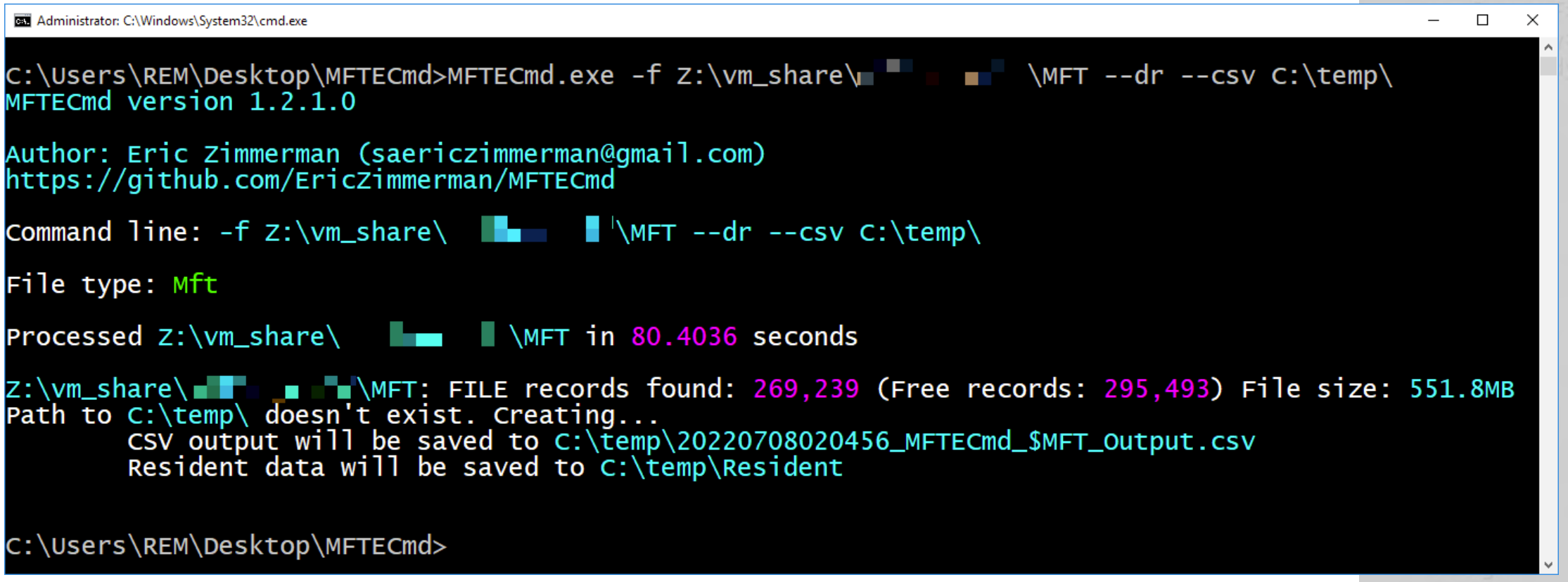
Real-World Example

- We at BlackBerry recently published an article on the "MONTI strain" ransomware group (for528.com/monti)
- MONTI used the Action1 RMM, which was a new TTP
- During the IR, I was able to recover the file you see here from an $MFT file
- This file contained the MONTI actor's Action1 Customer ID! – Thanks, MFTEcmd!



MFTEcmd **DEMO**

Nothin' better than a DEMO!



ResponderCon

Questions/Comments?

THANK YOU!!!

Have Fun with It!:
Tracking Ransomware Operator Lateral Movement and Recovering Deleted Files the *Easy Way*!

Ryan Chapman | **@rj_chap**

ResponderCon