

# Log Analysis Ain't Just for Lumberjacks

Data analytics for Purple Teams and Red Team Post-mortem

Corey Thuen  
Co-Founder, Gravwell  
@coreythuen



A system is "good" if it does what it's supposed to do, and "secure" if it doesn't do anything else.

Dr. Eugene "Spaf" Spafford

Security is a process, not a product.

Bruce Schneier



User phished

**Custom** Malware downloaded and executed via chrome

- Port scan local subnets
- Exfiltrate port scan results over DNS
- Copy itself to fileshares
- Rename copy to name from list of enticing filenames

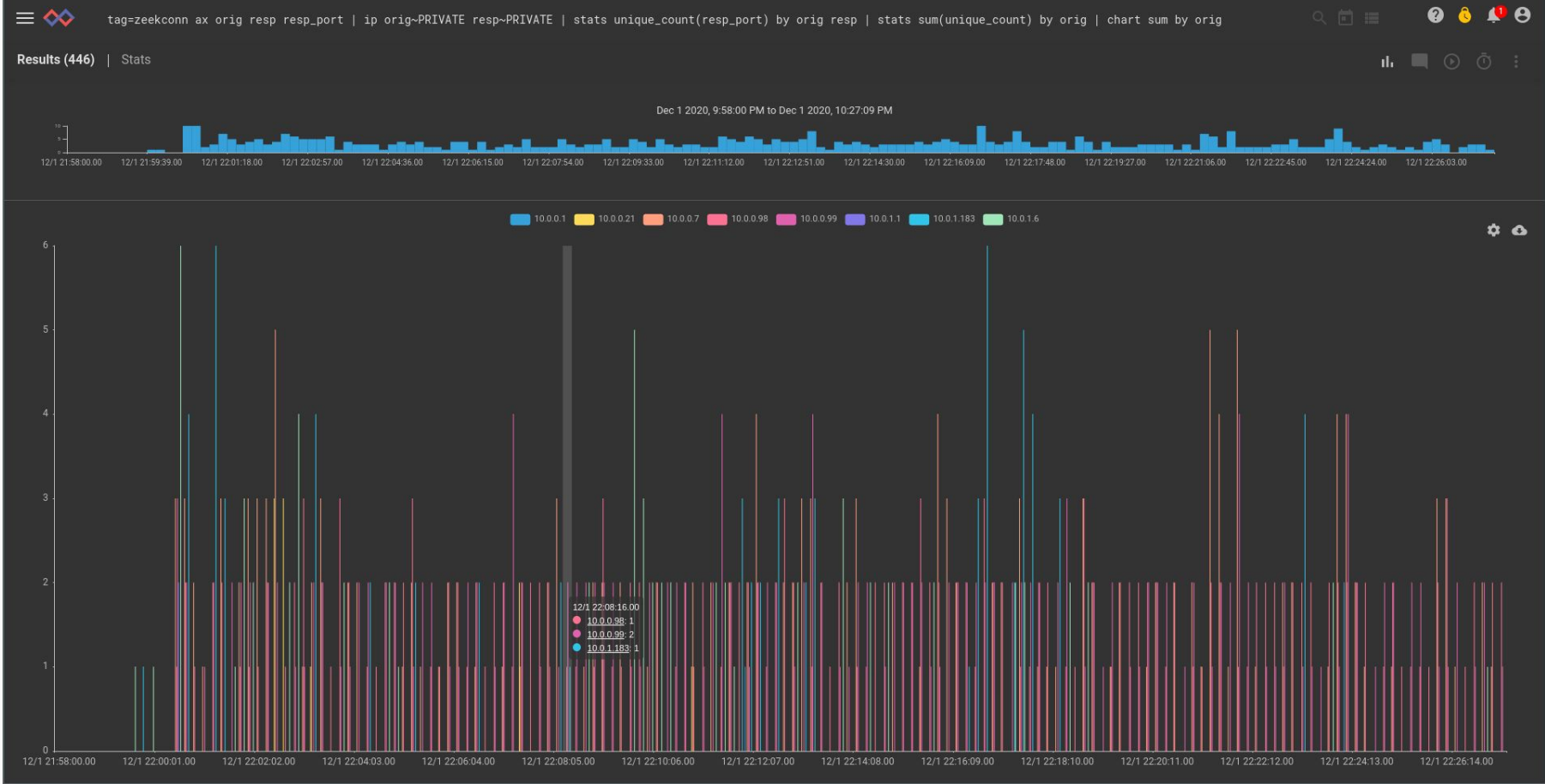
Malware executed by different user via fileshare

The image is a composite of three screenshots illustrating a malicious activity sequence:

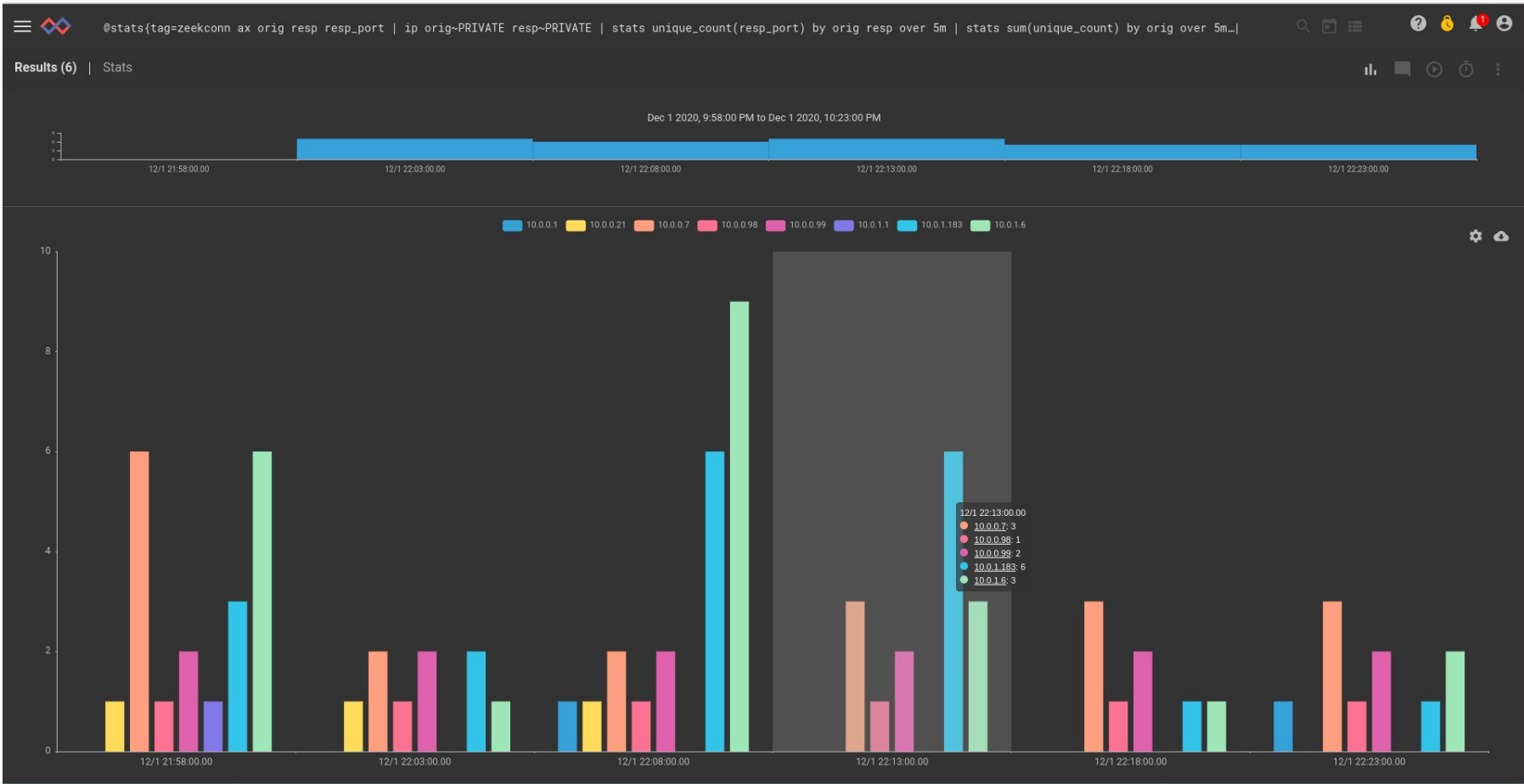
- Top Left:** A browser window showing the index of a directory named `/cutepuppies`. The index lists files with columns for Name, Last modified, Size, and Description. The files listed are:

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">totallynotmalware.bin</a>	2020-11-27 10:43	6.6M	
<a href="#">totallynotmalware.exe</a>	2020-11-27 10:43	6.3M	
- Top Right:** A Windows File Explorer window showing the local `Downloads` folder. A file named `totallynotmalware` is highlighted, with a context menu open over it.
- Bottom:** A Windows File Explorer window showing a network share at `10.0.0.21`. The share contains folders for `games`, `Hades`, `robertpaulson pi`, and `savedgames`. A context menu is open over the `users` folder, indicating the malware is being executed via this share.

The Tip: Anomalous behavior  
by a host on the network.  
Fusion of weak signals.



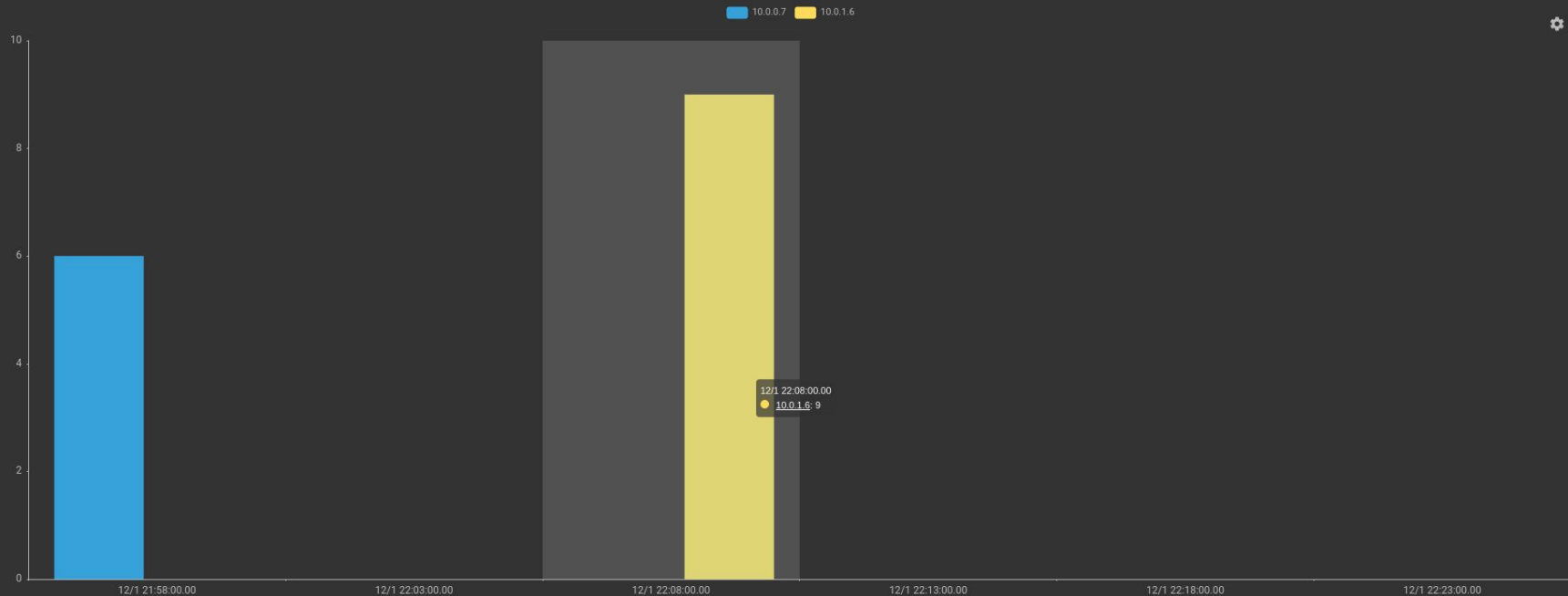
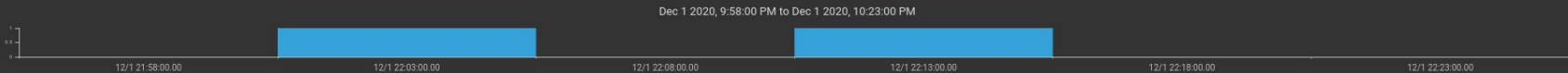
A basic aggregate chart of network connections from one intranet system to another



Modifying the query slightly we can create a chart of all new network connections originating from a given IP, bucketed into 5 minute windows

```
@stats{tag=zeekconn ax orig resp resp_port | ip orig~PRIVATE resp~PRIVATE | stats unique_count(resp_port) by orig resp over 5m | stats sum(unique_count) by orig over 5m...}
```

Results (2) | Stats

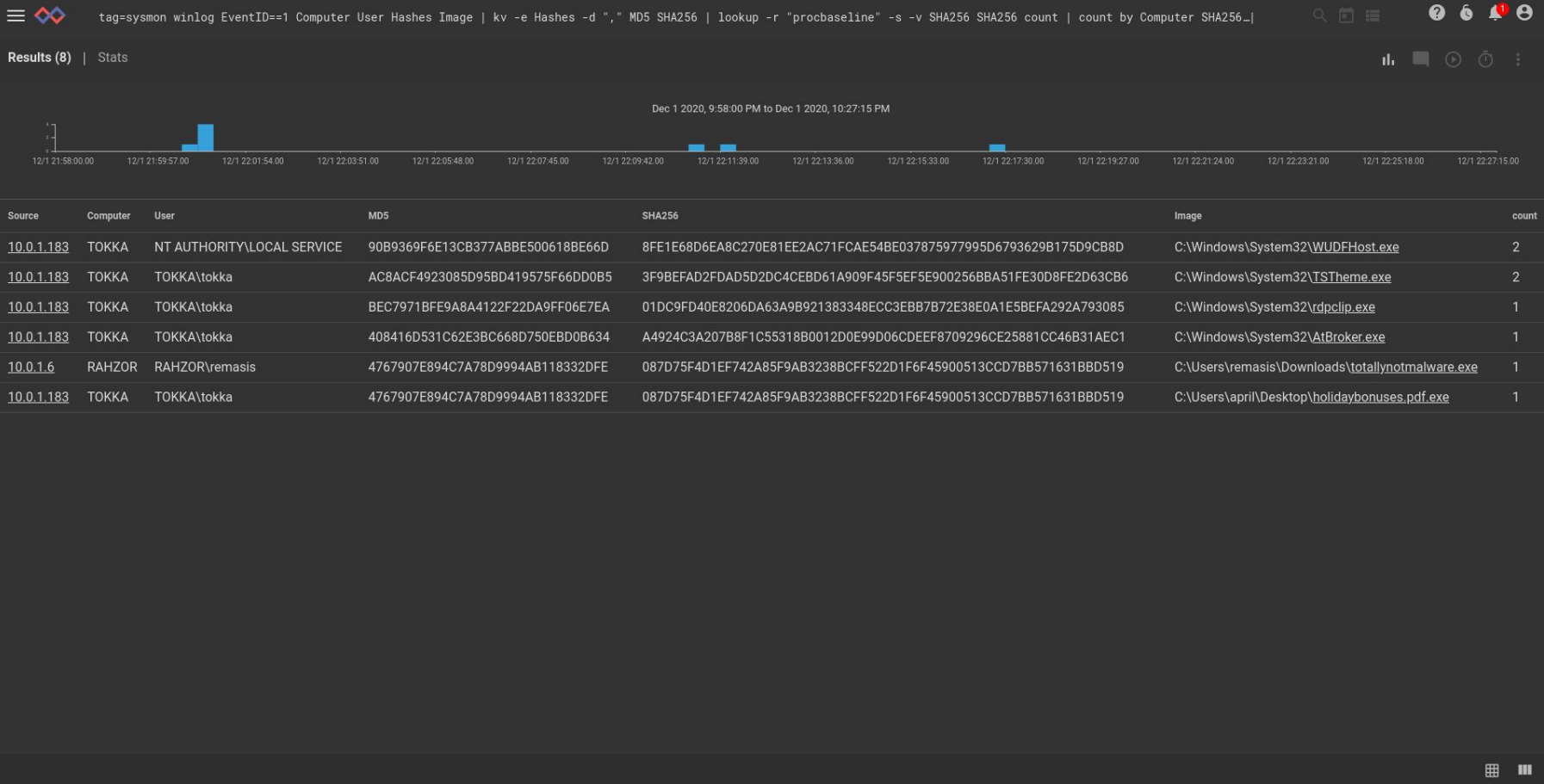


Commoditized data science means using understandable queries to establish statistical parameters on the fly and drop noise below the floor. Here we only show a 5 minute window that was 2 standard deviations from the mean.

Source	Corr	Actual query:	count
tag=sysmon winlog EventID==1 Computer User Hashes Image   kv -e Hashes -d ", " MD5 SHA256   count by Computer SHA256   table -save procbaseline SRC Computer User MD5 SHA256 Image count			
10.0.1.1 83	TOKKA	NT AUTHORITY\SYSTEM F745 D1E50A9	C:\windows\system32\taskhostw.exe 39
10.0.1.1 83	TOKKA	TOKKA\tokka 3C82D36C2B28EB036EFA4691DE85A3CD 4EE9D250485E383365FCF6DDEC48A03D197F94C40FCF23E13DEB4C226DF4A79	C:\Windows\System32\GameBarPresenceWriter.exe 1
10.0.1.1 83	TOKKA	TOKKA\tokka 97227A2485DB97C25AC4E17E8FC44E3B AB2FC49A85789EB6C0F7BCEA8570461043D8F7213F9325D5DE4BCD9016CC4127	C:\Program Files (x86)\Steam\bin\vulkandrivervquery.exe 3
10.0.1.1 83	TOKKA	TOKKA\tokka 259D746528A65ED5953E6294D8EC1507 40A86A19EF9AFA0021CA59D08454034E6A6C37D620BE583C26E05E1D55D11CA0	C:\Windows\System32\sihost.exe 2
10.0.1.1 83	TOKKA	NT AUTHORITY\SYSTEM 32113FBBC44A386234AE31994A066617 5CF2D2B0A600D8C783AD085A994B3D8E090425A0ECF49A923F435D56C20EFF4B	C:\Program Files\gravwell\eventlog\winevents.exe 1
10.0.1.1 83	TOKKA	NT AUTHORITY\SYSTEM CC25007DBB7A5F1F2F42C5487B97CCC2 E8CD4661B393A1A66E02257672F2940DE10A6EE8C06F9121A8787BFFC49AD430	C:\Windows\System32\upfc.exe 2
10.0.1.1 83	TOKKA	NT AUTHORITY\SYSTEM 23019322FFECB179746210BE52D6DE60 F2C7D894ABE8AC0B4C2A597CAA6B3EFE7AD2BDB4226845798D954C5AB9C9BF15	C:\Windows\System32\csrss.exe 3
10.0.1.1 83	TOKKA	TOKKA\tokka D5257453B232978C8E32E219E9B1F585 A2D3B3A53CA1CD5E43836977DA517B4E545C9C4DDBDFD8A429A21E426B65E827	C:\Program Files (x86)\Fantasy Grounds\FantasyGrounds.exe 3
10.0.1.1 83	TOKKA	TOKKA\tokka D6FD152DEA780FA5757874F7C0D89E9D1 5B742EF16D6EC58702809A0E5F816B0AA4E385F5343F8B75C5D88453274863F7	C:\Program Files\AMD\CIM\BIN64\InstallManagerApp.exe 2
10.0.1.1 83	TOKKA	NT AUTHORITY\LOCAL SERVICE 44B4D47F3DD5DA2E4EE0B328E7F2DC8 F07E5BA7FEEB9A18810D72E6A3A9B769C5A3D88064D71F92784FC8EA0F22491A	C:\Windows\System32\dashost.exe 2
10.0.1.1 83	TOKKA	TOKKA\tokka 87414DA665DB6B52BC1E51A6166E357D 12FAF6D31338B40691C5D433F2BCFE54899A58B8A8E8FA6B673FA5F3E82A0AA7	C:\Windows\System32\SecurityHealthHost.exe 1
10.0.1.1 83	TOKKA	NT AUTHORITY\SYSTEM 3C112A2CCE8308809A68FB1C7F6B0291 EB99368D022521E05657CA15884BA078ABDF216F2C92CFAA5E97BC2ECA5EBA23	C:\Windows\System32\mitigationscanner.exe 1
10.0.1.1 83	TOKKA	NT AUTHORITY\SYSTEM 61E5C6A186ECCFBFA1238DCB8A35BFC3 705D416C777A04B0EF8BB836E98B65F1DE16D02D2C434A480A8956D9A07A873B	C:\Windows\System32\SIHClient.exe 1
10.0.1.1	TOKKA	TOKKA\tokka 5EA16F52FF91DCC13ED00CA59879 F2326735452AC846B8D942D4F84C9318E84E7058BC1AC9E3DE0BED88A	C:\Windows\System32\leathe.exe 1

Process whitelisting results in a lot of noise, but it can be a useful weak signal for fusion. Let's create a list from the previous 24 hours. We could automate this search to make it a rolling whitelist.





Using the whitelist, we can create a list of new process executables.

# Combined weak signals become strong



At least 1 host is present in both weak signals

We could add more weak signals for higher fidelity

We walked through this manually here, but we could automate or combine into a single dashboard to automate mundane parts of threat hunting.

# Hypothesis

Hypothesis - 10.0.1.6 is "funny lookin'"

Around 12/1 22:08, 10.0.1.6 had unusual network activity caused by never-before-seen process.

Hypothesis: "totallynotmalware.exe" is malware.

