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

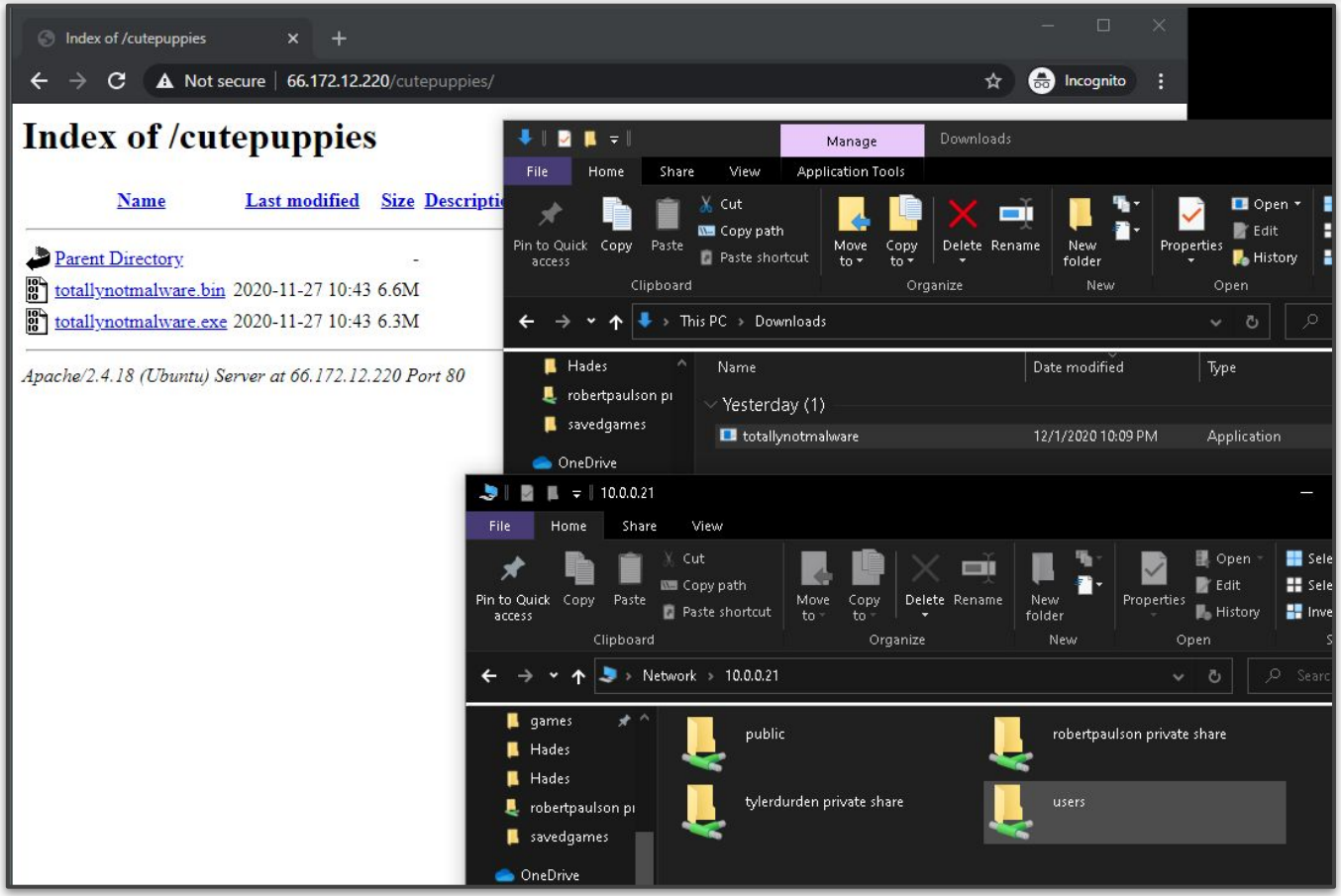
Malicious Activity Prologue

User phished

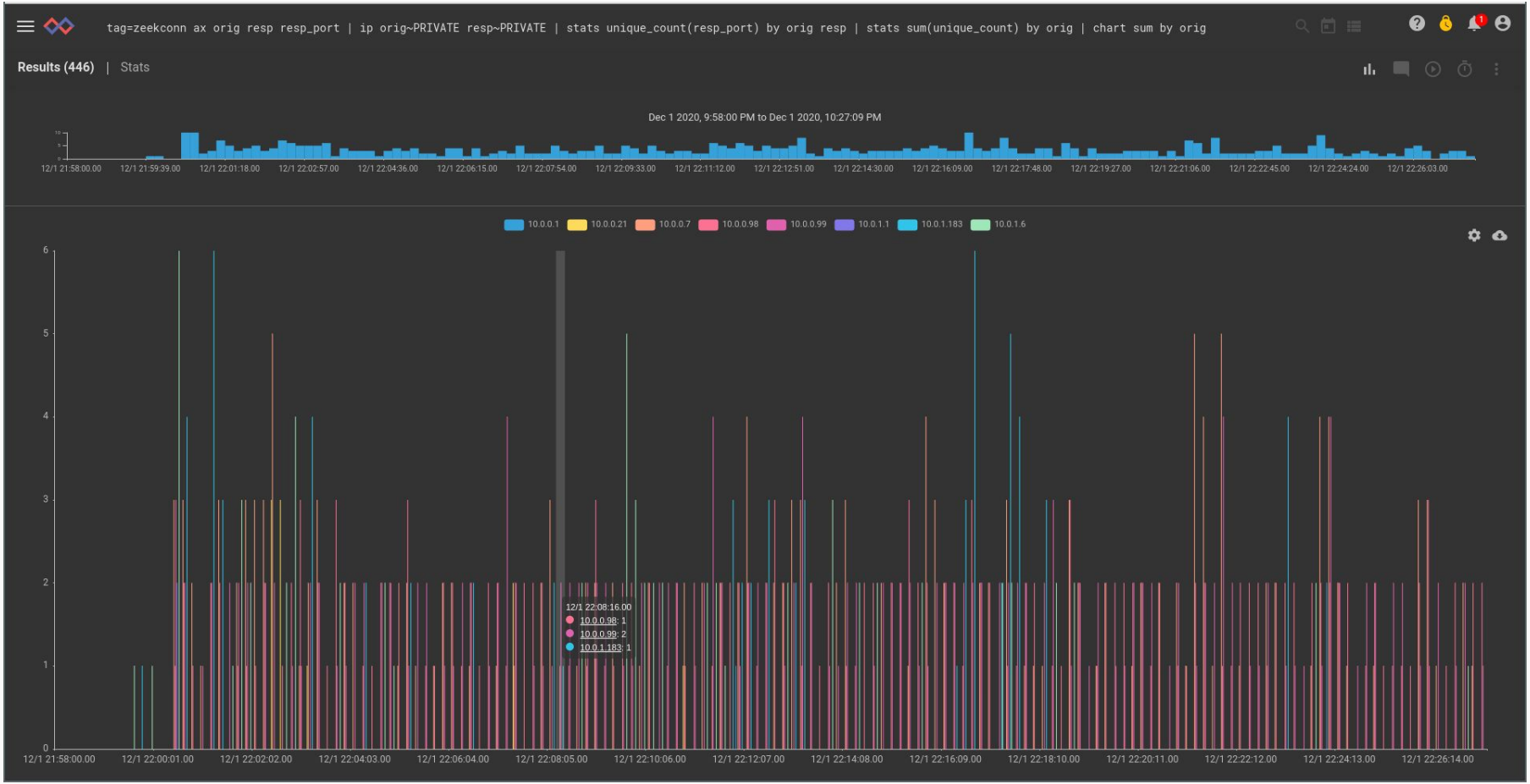
Custom Malware downloaded and executed via chrome

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

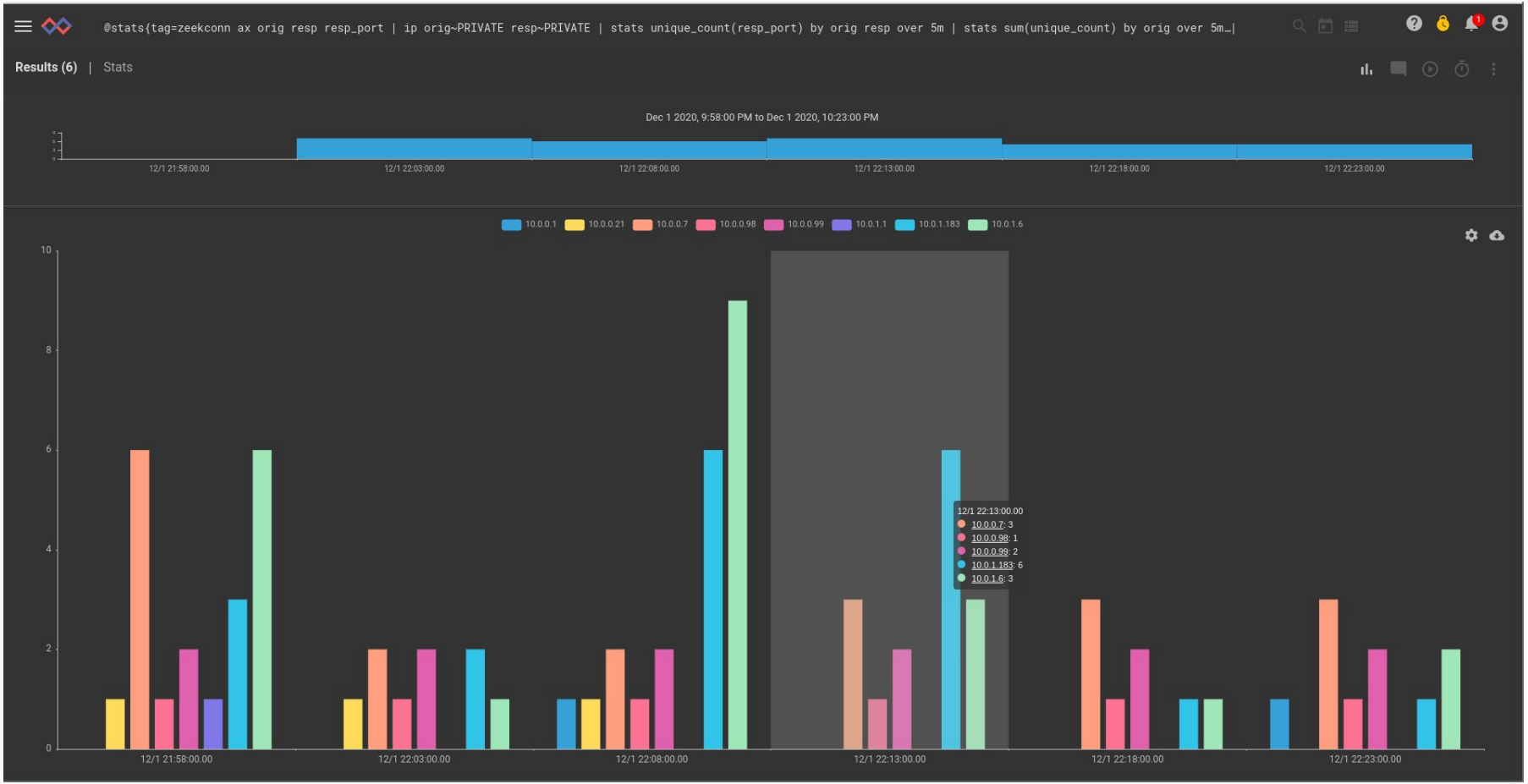
Malware executed by different user via fileshare



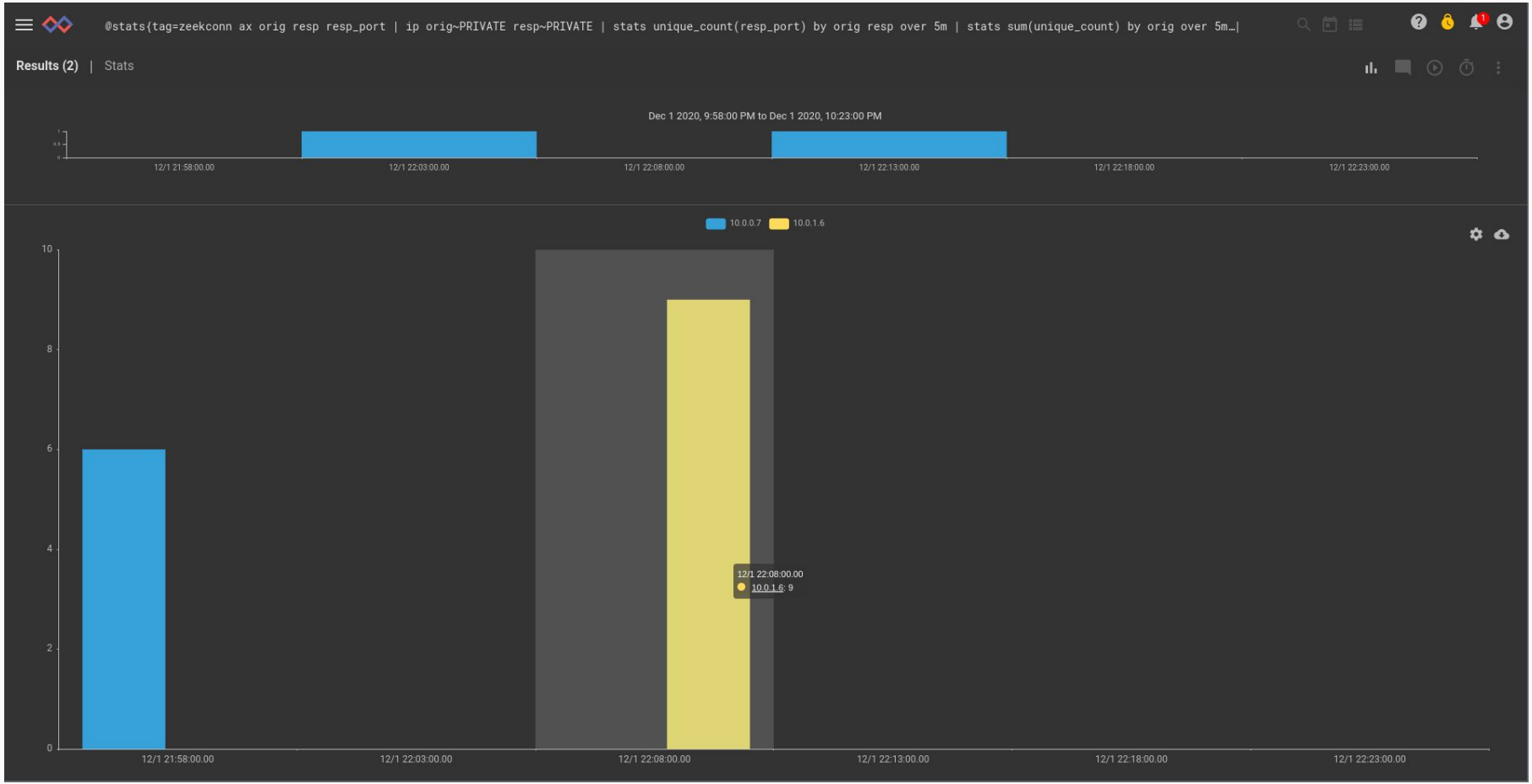
The Tip: Anomalous behavior by a host on the network. Fusion of weak signals.



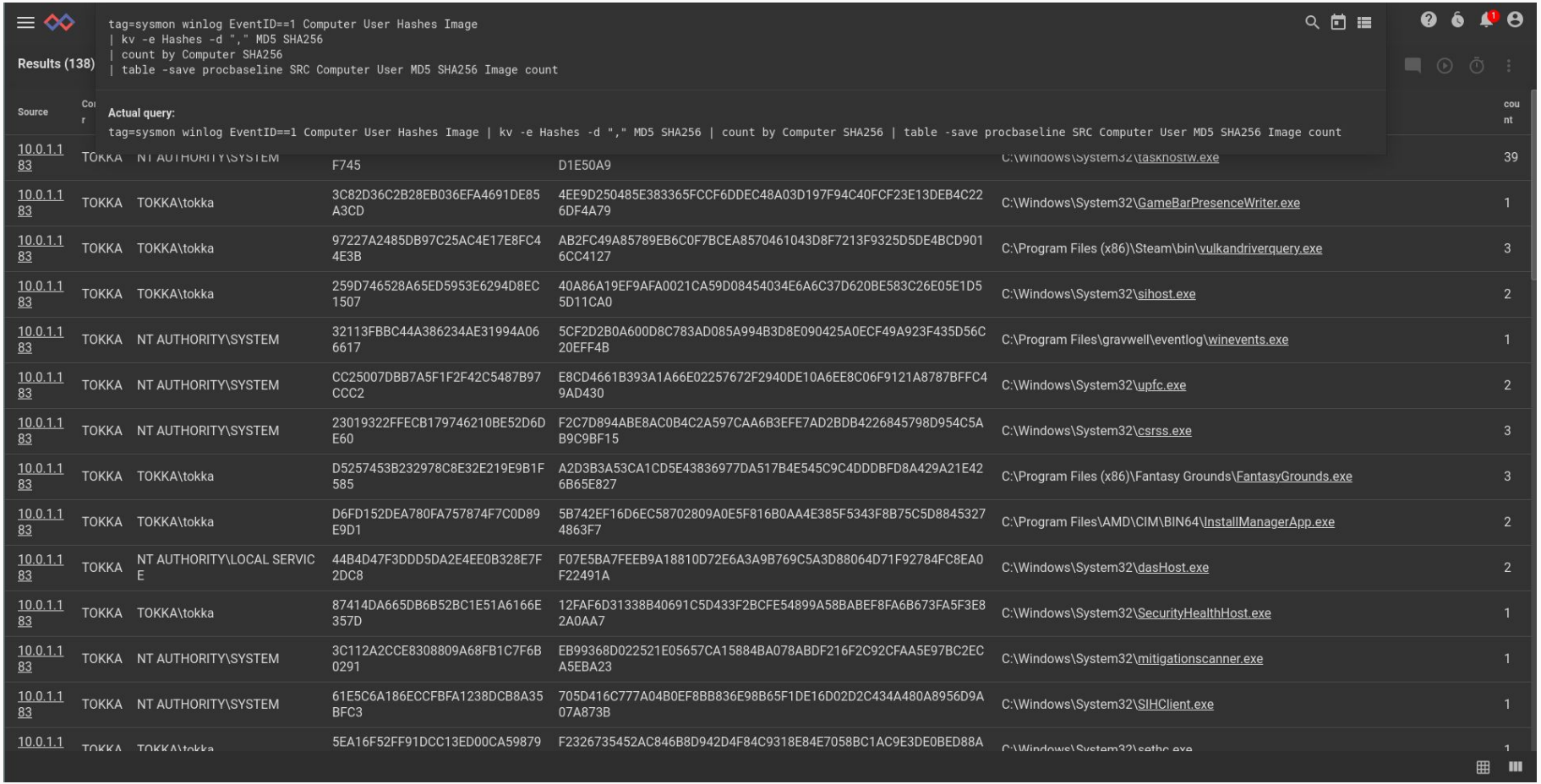
A basic aggregate chart of network connections from one intranet system to another



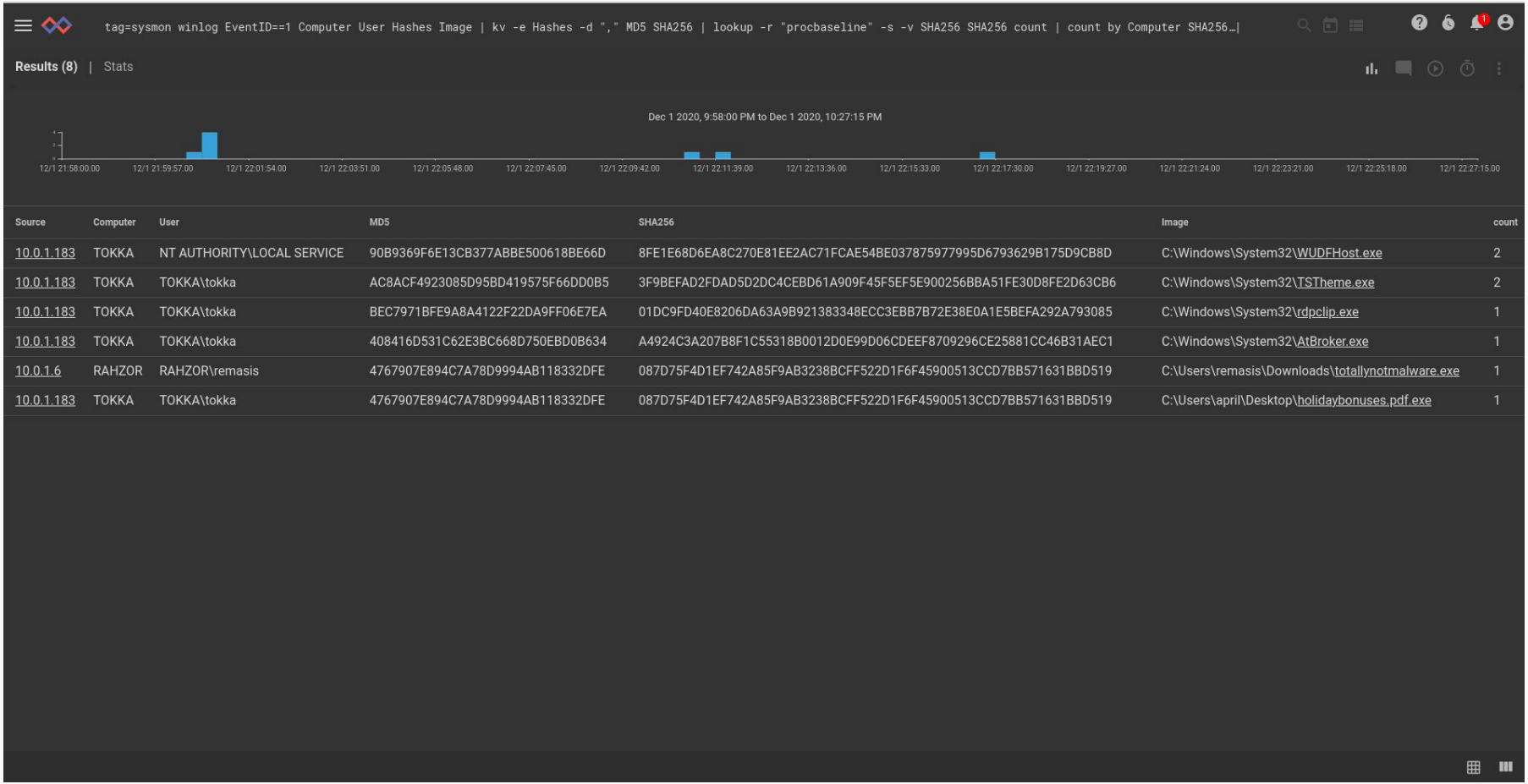
Modifying the query slightly we can create a chart of all new network connections originating from a given IP, bucketed into 5 minute windows



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.



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.



Source	Computer	User	MD5	SHA256	Image	count
10.0.1.183	TOKKA	NT AUTHORITY\LOCAL SERVICE	90B9369F6E13CB377ABBE500618BE66D	8FE1E68D6EA8C270E81EE2AC71FCAE54BE037875977995D6793629B175D9CB8D	C:\Windows\System32\WUDFHost.exe	2
10.0.1.183	TOKKA	TOKKA\tokka	AC8ACF4923085D95BD419575F66DD0B5	3F9BEFAD2FDAD5D2DC4CEBD61A909F45F5EF5E900256BBA51FE30D8FE2D63CB6	C:\Windows\System32\TSTheme.exe	2
10.0.1.183	TOKKA	TOKKA\tokka	BEC7971BFE9A8A4122F22DA9FF06E7EA	01DC9FD40E8206DA63A9B921383348ECC3EBB7B72E38E0A1E5BEFA292A793085	C:\Windows\System32\rdpclip.exe	1
10.0.1.183	TOKKA	TOKKA\tokka	408416D531C62E3BC668D750EBD0B634	A4924C3A207B8F1C55318B0012D0E99D06CDEEF8709296CE25881CC46B31AEC1	C:\Windows\System32\AtBroker.exe	1
10.0.1.6	RAHZOR	RAHZOR\remasis	4767907E894C7A78D9994AB118332DFE	087D75F4D1EF742A85F9AB3238BCFF522D1F6F45900513CCD7BB571631BBD519	C:\Users\remasis\Downloads\totallynotmalware.exe	1
10.0.1.183	TOKKA	TOKKA\tokka	4767907E894C7A78D9994AB118332DFE	087D75F4D1EF742A85F9AB3238BCFF522D1F6F45900513CCD7BB571631BBD519	C:\Users\april\Desktop\holidaybonuses.pdf.exe	1

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.