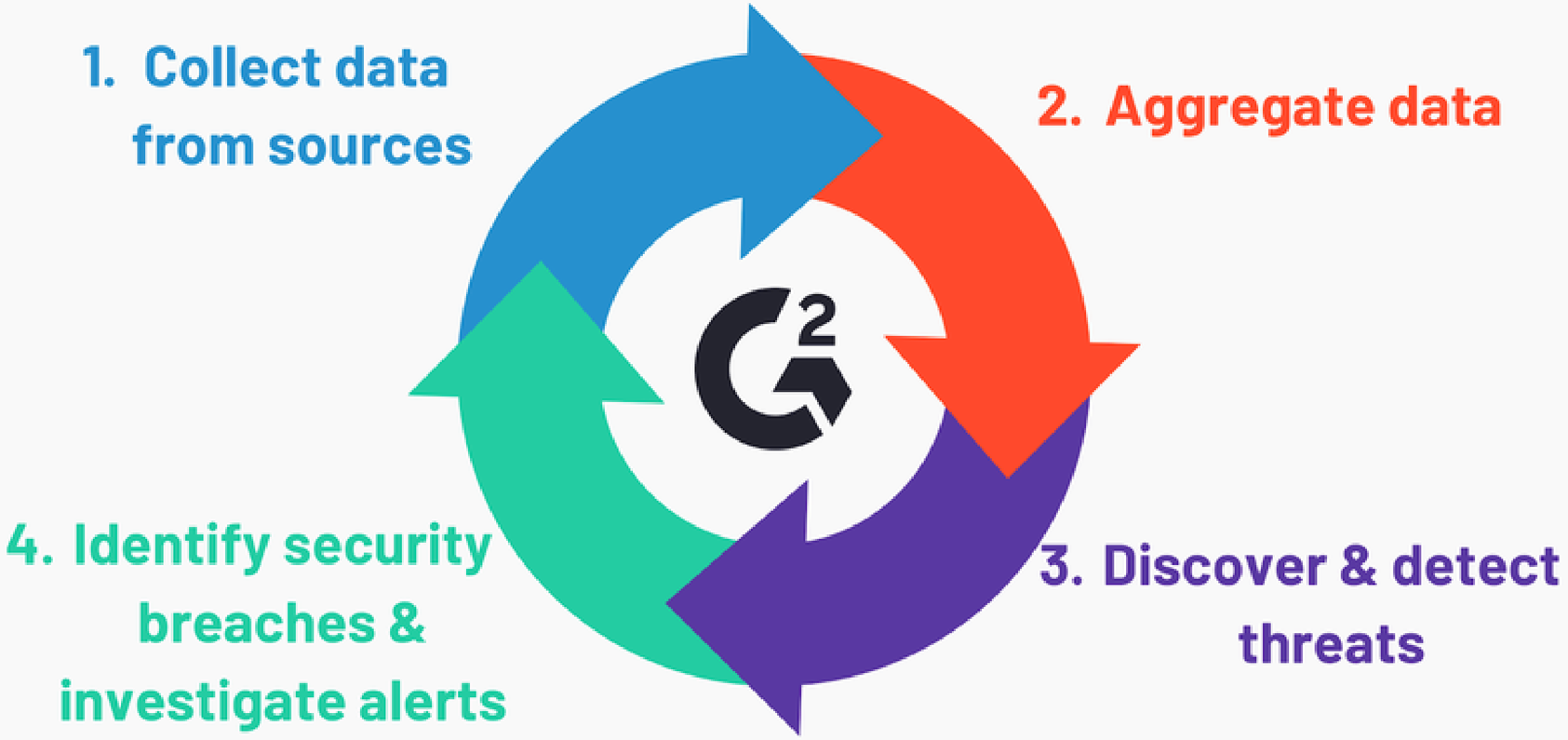
SPLUNK SECURITY FUNDAMENTALS

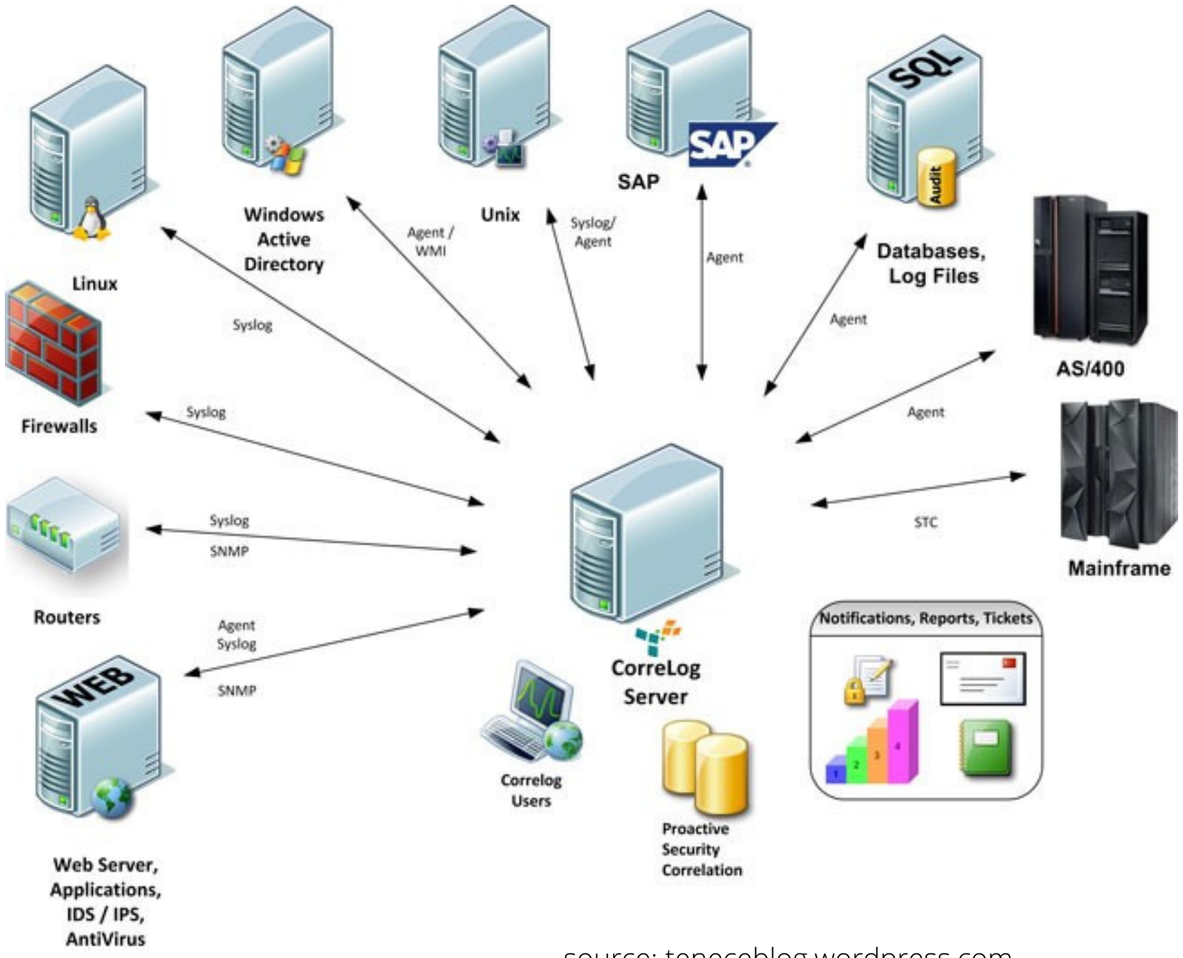
Ali Alwashali

The SIEM Process



COLLECT DATA

- Eevent Logs
- Registry
- Network Activitiy
- Firewall deny and permit logging
- Web server logs
- IDS logs
- Application logs



source: teneceblog.wordpress.com

Network Data Collection

Network Security Monitoring Tool

intrusion detection
& intrusion prevention system

Endpoint Logs

Windows 10

Registry

Event log

Sysmon

Sysmon provides a pretty detailed monitoring of operating system activity, starting from process monitoring, going through monitoring all the network and ending up with a discovery of the different types of exploitation techniques.

Sysmon - Windows Sysinternals

Monitors and reports key system activity via the Windows event log.

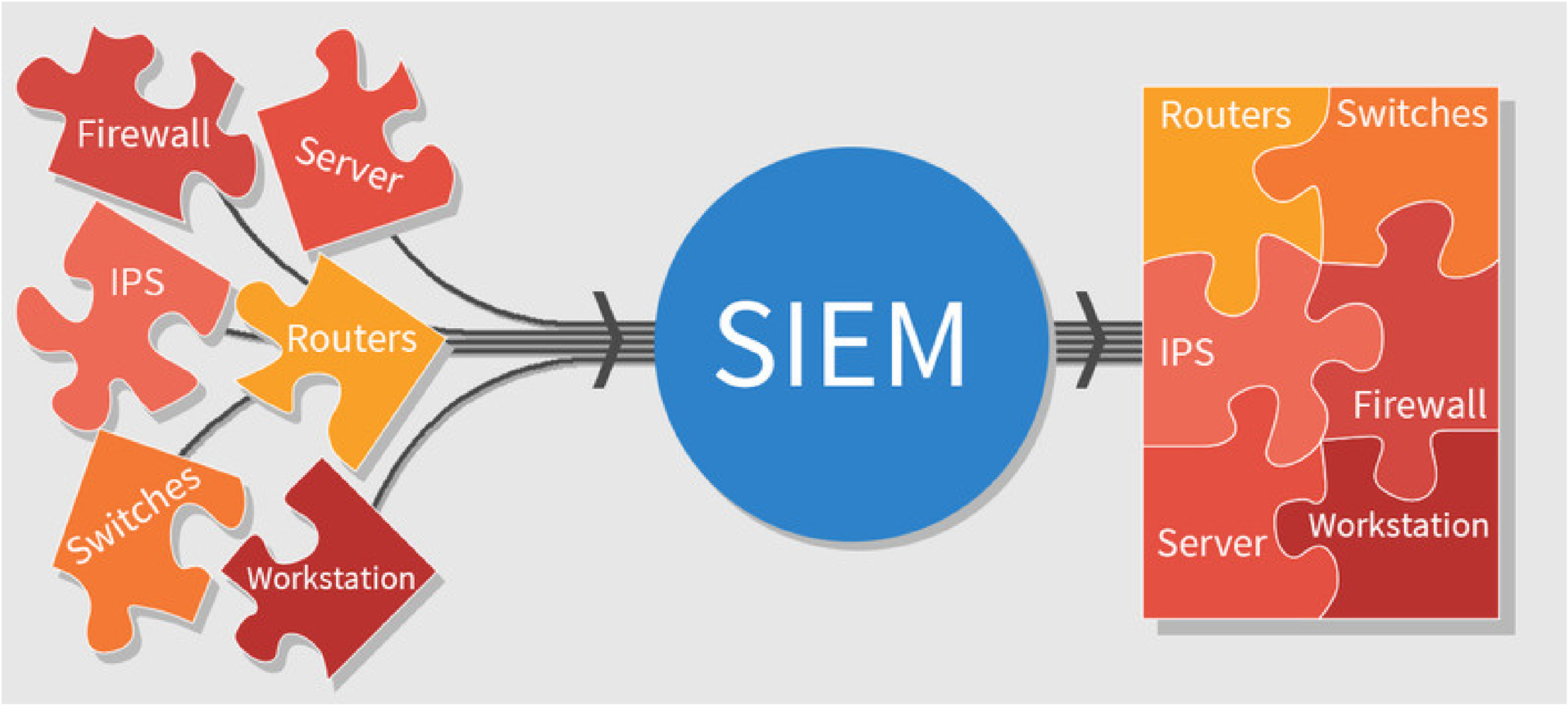
docsmsft / markruss

SIEM Agents

IBM QRadar → Wincollect

splunk> → Universal forwarder

elastic → Winlogbeat

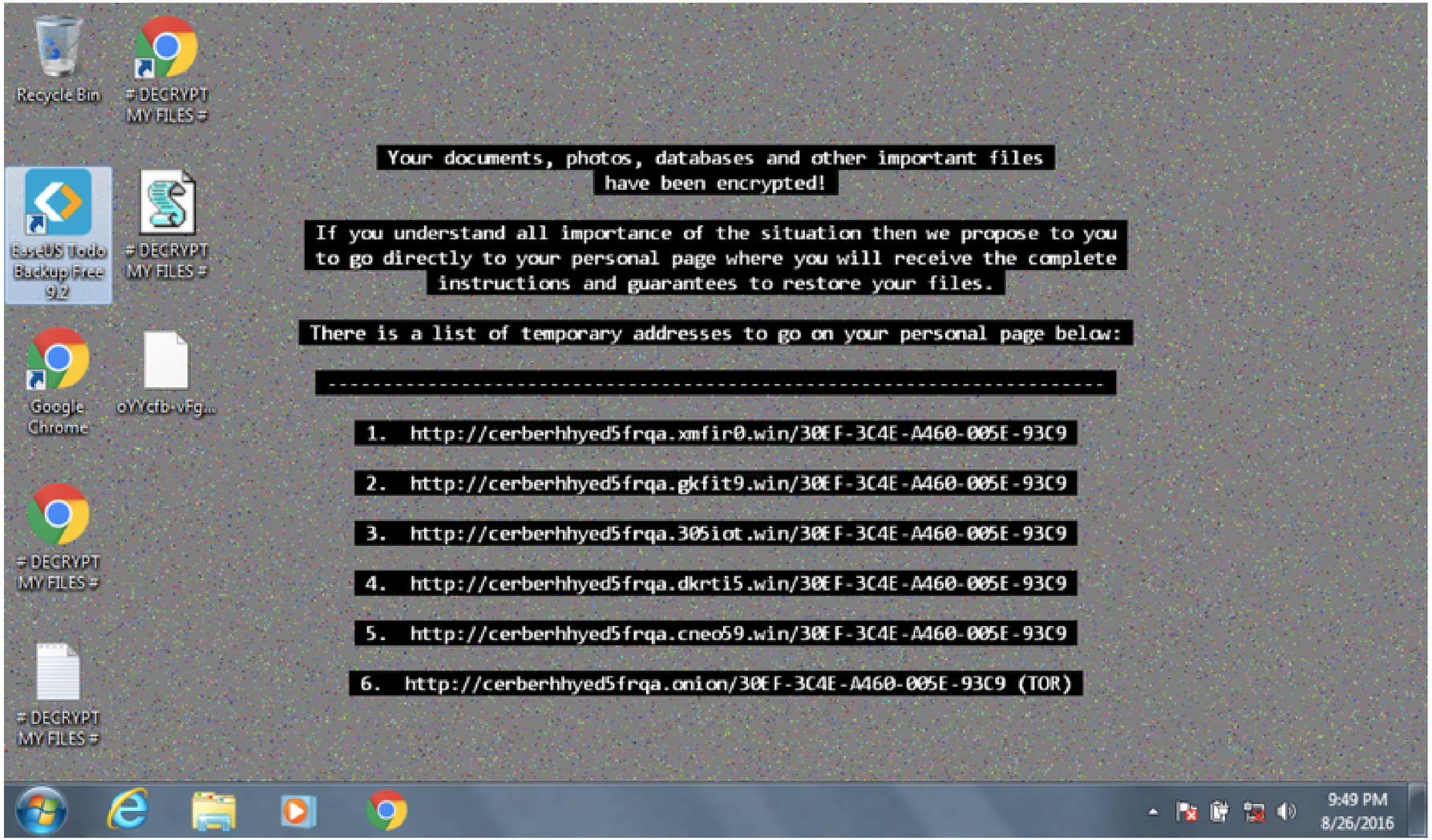

Firewall
Server
IPS
Routers
Switches
Workstation
SIEM
Routers
Switches
IPS
Firewall
Server
Workstation

Demo

splunk>

Download: https://cyberdefenders.org/labs/15

Ransomware Infection



Ransomware Infection

- What is the malware family?
- What caused the infection?
- Where did the malware come from?
- How many files were encrypted?
- How many computers infected ?

You have been given only timestamp and hostname

2016-08-24 16:43:00

we8105desk

What is the malware family?

- Ransomware picture
- Suricata signatures

index=botsv1 sourcetype=suricata src_ip=192.168.250.100

How we8105desk was infected?

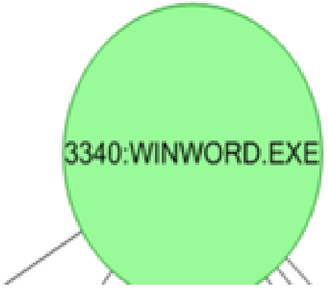
Know more about the malwre. Start with Google

attack cycle, Exploit Guard provides coverage for most steps of the attack cycle – beginning in this case at the second step.

The most common way to deliver ransomware is via Word documents with embedded macros or a Microsoft Office exploit. FireEye Exploit Guard detects both of these attacks at the initial stage of the attack cycle.

PowerShell Abuse

When the victim opens the attached Word document, the malicious macro writes a small piece of VBScript into memory and executes it. This VBScript executes PowerShell to connect to an attacker-controlled server and download the ransomware (profilest.exe), as seen in Figure 1.



How we8105desk was infected?

Use Sysmon to search for an MS-Word execution

```
index=botsv1 host=we8105desk winword.exe sourcetype="XmlWinEventLog:MicrosoftWindowsSysmon/Operational" EventCode=1
```

How we8105desk was infected?

Answer:

User opend malicious file from pen drive

MD5 ▾	AD7B9C14083B52BC532FBA5948342B98
Opcode ▾	0
ParentCommandLine ▾	"C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm"
ParentImage ▾	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE
ParentProcessGuid ▾	{0F2D76F0-CEA0-57BD-0000-00108D2B3000}
ParentProcessId ▾	3756
ProcessGuid ▾	{0F2D76F0-CEA9-57BD-0000-001037FE3000}

What is the name of the USB drive ?

index=botsv1 sourcetype=winregistry friendlyname | table _time host object data

host	object	data
we8105desk	friendlyname	MIRANDA_PRI
we8105desk	friendlyname	MIRANDA_PRI

How many .txt files were encrypted?

We need to know the name of the process responsible for encryption

```
index=botsv1 host=we8105desk sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1  | table _time process_name cmdline parent_process ParentCommandLine | reverse
```

wscript.exe
https://attack.mitre.org/techniques/T1059/005/

How many .txt files were encrypted?

Processes of interest : osk, 121214, cmd

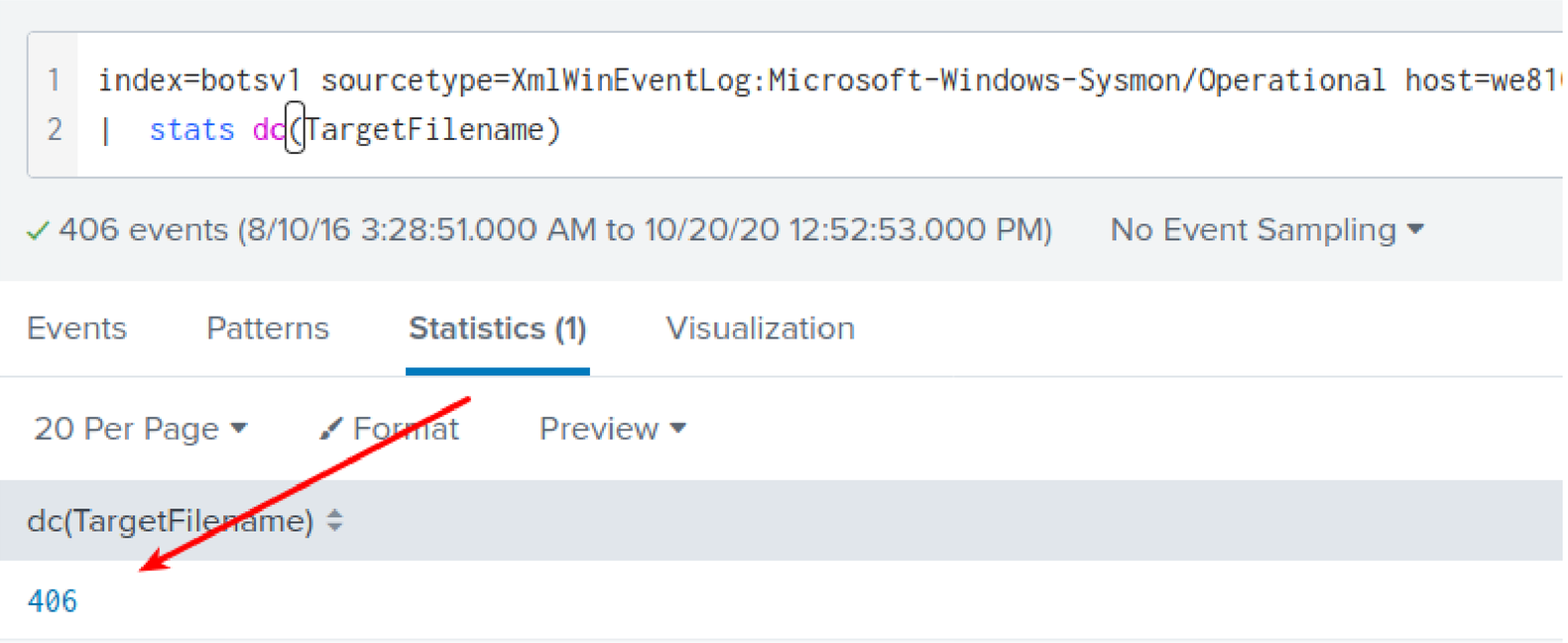
```
index=botsv1 host=we8105desk sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" (process_name="cmd.exe" OR process_name="osk.exe" OR process_name="121214.tmp")
```

```
index=botsv1 host=we8105desk sourcetype="XmlWinEventLog:Microsoft-WindowsSysmon/Operational" (process_name="cmd.exe" OR process_name="osk.exe" OR process_name="121214.tmp") | stats count by EventCode process_name | sort count | reverse
```

Check event ID, path, process name

How many .txt files were encrypted?

index=botsv1 sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational host=we8105desk EventCode=2 TargetFilename="C:\\Users\\bob.smith.WAYNECORPINC*.txt" | stats dc(TargetFilename)

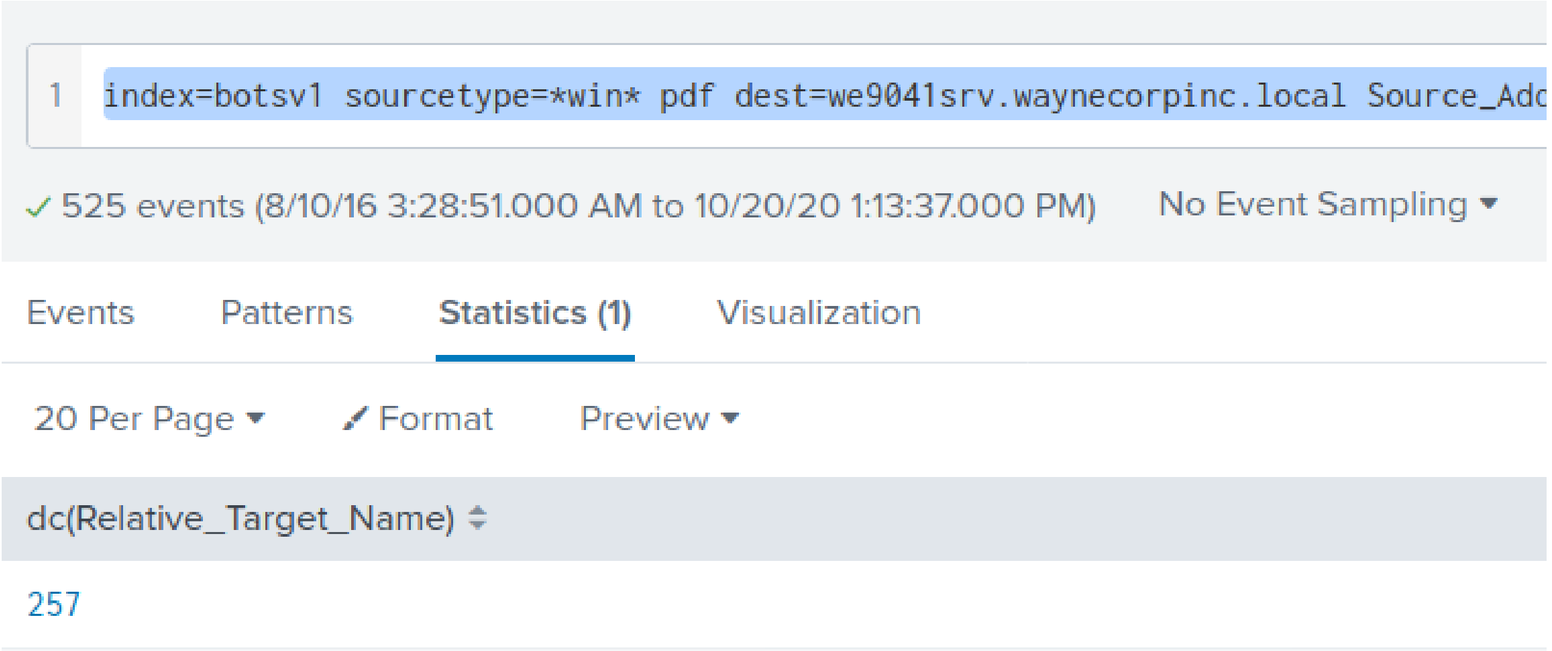


How many computers were infected ?

In most cases, ransomware encrypts files shared with the infected machine. We need to know if there are shares available

index=botsv1 sourcetype=winregistry host=we8105desk Mountpoints2

object	##192.168.250.20#fileshare
object_category	registry
object_path	HKU\s-1-5-21-67332772-3493699611-3403467266-1109\software\microsoft\windows\currentversion\explorer\mountpoints2\##192.168.250.20#fileshare
pid	3496
process_image	c:\Windows\explorer.exe



index=botsv1 sourcetype=*win* pdf dest=we9041srv.waynecorpinc.local Source_Address=192.168.250.100 EventCode=5145 action=success *.pdf | stats dc(Relative_Target_Name)

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5145

Where did the malware come from?

We can check the domain names requests directly after execution of the malware, 2016-08-24 16:43:21

```
index=botsv1 sourcetype=stream:DNS src=192.168.250.100 record_type=A
|  table _time query
```

```
index=botsv1 source="stream:http"
```

https://www.netskope.com/blog/anatomy-ransomware-attack-cerber-uses-steganography-hide-plain-sight

Website Defacement

Website Defacement

imreallynotbatman.com was defaced by a hacker

Your job is to find out the root cause of the incident

Answer following question

- What is the vulnerability?
- What is the tool used?

Website Defacement

Logical step is to study what data available about imreallynotbatman.com

index=botsv1 imreallynotbatman.com

Narrow down the search to website ip and domain name only

index=botsv1 dest=imreallynotbatman.com OR dest_ip="192.168.250.70"

Website Defacement

Suricata alerts

Top 10 Values	Count	%
ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	103	19.656%
GPL WEB_SERVER 403 Forbidden	51	9.733%
ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	48	9.16%
ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.	41	7.824%
SURICATA HTTP Host header invalid	35	6.679%
ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	33	6.298%
ET WEB_SERVER SQL Injection Select Sleep Time Delay	32	6.107%
ET WEB_SERVER Possible CVE-2014-6271 Attempt	18	3.435%
ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	18	3.435%
ET WEB_SERVER PHP tags in HTTP POST	13	2.481%

Website Defacement

From above alerts, probably, an automated attack using a scanner

Aks me **Why** ?

What type of web Applicatin

index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70"

index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" status=200

/joomla/index.php/component/search/
/joomla/administrator/index.php
/joomla/index.php
/
/joomla/agent.php
/windows/win.ini
/joomla/media/jui/js/jquery-migrate.min.js
/joomla/media/jui/js/jquery-noconflict.js
/joomla/media/jui/js/bootstrap.min.js
/joomla/media/system/js/html5fallback.js
/joomla/templates/protostar/js/template.js

Joomla!®

From what we know about web apps, joomla particularly, the HTTP requests are anomalous

Web traffic anomaly investigation

```
index=botsv1 sourcetype=stream:http  dest_ip="192.168.250.70" http_method=po
```

```
index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70"
http_method=post form_data=*username*passwd*
```

```
index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70"
 http_method=post form_data=*username*passwd* | rex field=form_data
"passwd=(?<userpassword>\w+)" | table userpassword
```

Move backword and forward in the cyber kill chain to find the messing pieces

Process execution on the server

```
index=botsv1 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host=we1149srv signature_id=1
```

```
index=botsv1 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host=we1149srv signature_id=1 |stats count by process_name
```

```
index=botsv1 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
host=we1149srv signature_id=1 |table _time process_name process_id cmdline
ParentCommandLine parent_process_id
| reverse
```

WmiPrvSE.exe	3668	C:\Windows\system32\wbem\wmiprvse.exe -Embedding	C:\Windo DcomLaun
cmd.exe	2896	cmd.exe /c "3791.exe 2>&1"	"C:\Prog cgi.exe"
conhost.exe	3680	\??\C:\Windows\system32\conhost.exe 0xffffffff	cmd.exe
3791.exe	3880	3791.exe	cmd.exe
cmd.exe	3620	C:\Windows\system32\cmd.exe	3791.exe
conhost.exe	2248	\??\C:\Windows\system32\conhost.exe 0xffffffff	C:\Windo
net.exe	3900	net view /domain	C:\Windo
whoami.exe	3808	whoami	C:\Windo
net.exe	612	net share	C:\Windo
net1.exe	1984	C:\Windows\system32\net1 share	net sha
net.exe	2656	net session	C:\Windo
net1.exe	2608	C:\Windows\system32\net1 session	net ses

index=botsv1 3791.exe sourcetype="stream:http"

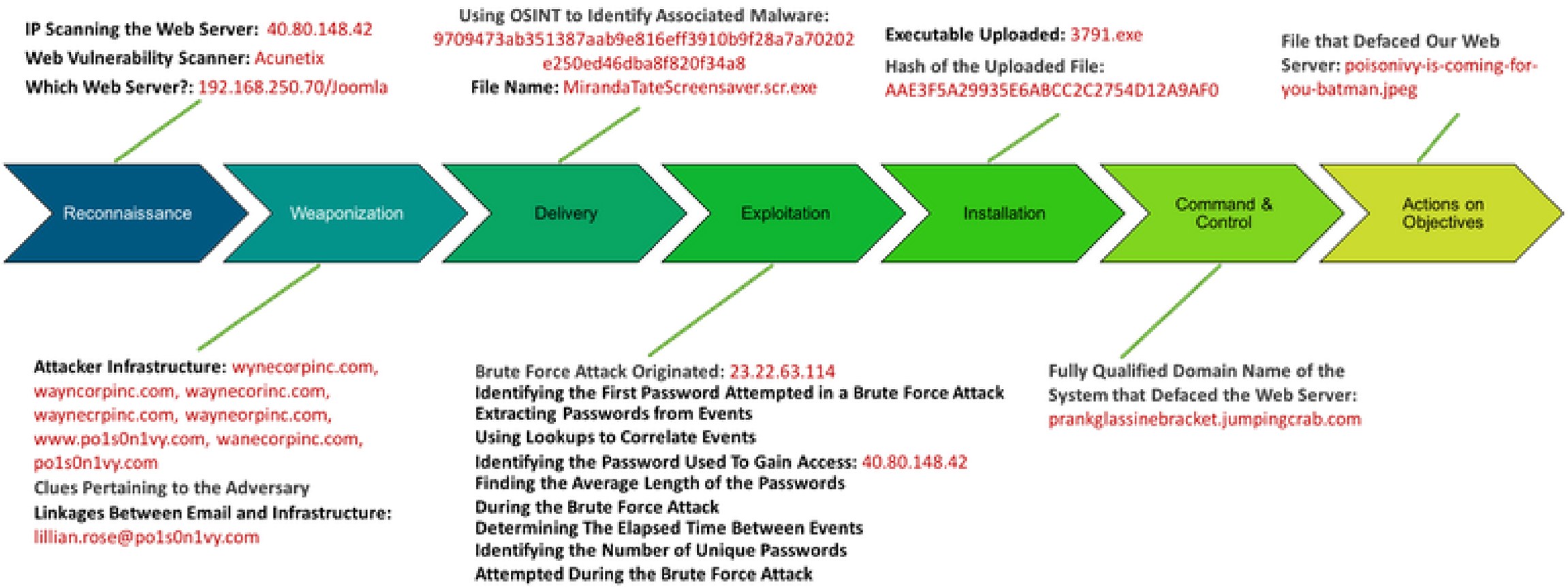

```
is_writable':true,'is_chmodable':true,'is_readable':true,'is_deletable':true,'is_editable':fa
,'size':'0 B','type':'Directory','modified':'2016\\/08\\/09 11:12','perms':'777 (rwxrwxrwx)',
table':true,'is_editable':false,'icon':'http:\\/\\/imreallynotbatman.com\\/joomla\\/administra
12','perms':'777 (rwxrwxrwx)','owner':'n\\/a'},{'name':'cli','is_file':false,'is_archive':fals
man.com\\/joomla\\/administrator\\/components\\/com_extplorer\\/images\\/extension\\/folder.pr
'is_file':false,'is_archive':false,'is_writable':true,'is_chmodable':true,'is_readable':true,
er\\/images\\/extension\\/folder.png','size':'4 KB','type':'Directory','modified':'2016\\/08\
dable':true,'is_readable':true,'is_deletable':true,'is_editable':false,'icon':'http:\\/\\/imre
```

File responsible for defacing the web site

index="botsv1" src=192.168.250.70 sourcetype=stream:http

Values	Count	%
http://prankglassinebracket.jumpingcrab.com:1337:1337/poisonivy-is-coming-for-you-batman.jpeg	2	25%
http://update.joomla.org/core/list.xml	2	25%
http://update.joomla.org/jed/list.xml	2	25%
http://update.joomla.org/core/extensions/com_joomlaupdate.xml	1	12.5%
http://update.joomla.org/language/translationlist_3.xml	1	12.5%

Attack Scenario



Resources:
https://cyberpolygon.com/materials/threat-hunting-why-might-you-need-it/
https://cyberpolygon.com/materials/threat-hunting-in-action/
https://cyberpolygon.com/materials/hunting-for-advanced-tactics-techniques-and-procedures-ttps/