Detect lateral movement in Windows environment with Suricata

Éric Leblond

Co Founder & CTO

STAMUS NETWORKS

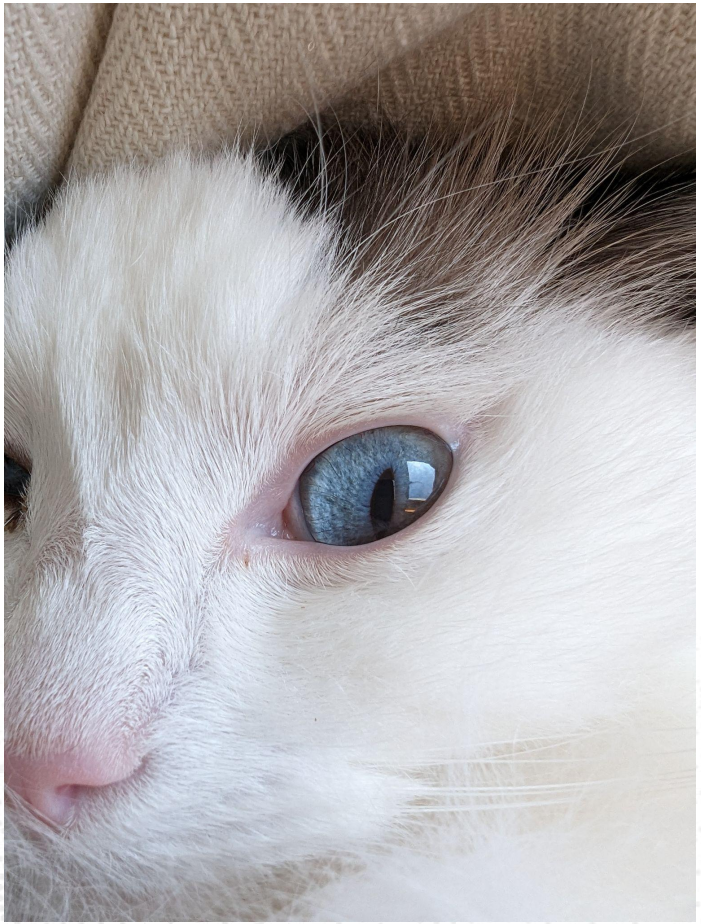
Who am I ?

Eric Leblond

- French
- Co founder & CTO of Stamus Networks
- Member of OISF's board
- Contributor to Suricata since 2009
- Co-author of "The Security Analyst's Guide to Suricata"

Stamus Networks:

- Editor of a Suricata based NDR solution
- Contributor to Suricata



Plan of talk

- Introduction to Suricata
- Objectives of the talk
- Tools used
- Discovering environment
- Lateral movement

Introduction to Suricata

One engine to rule them all

STAMUS NETWORKS

Suricata is far more than an IDS/IPS

Network Traffic
Cloud & On-premise

IDS Alerts

Protocol
Transactions

Network
Flows

PCAP
Recordings

Extracted
Files

Source: Stamus Networks

STAMUS NETWORKS

Suricata: a threat detection engine

- Born: 2010
- Weight: 600000 lines of code
- Composition: C, Rust
- Eat: live packets and dead ones
- Produce: JSON files/output
  - Protocol transaction
  - IDS alerts
  - PCAP
- Characteristics:
  - High speed
  - Open Source
  - Community driven
  - World famous

Open Information Security Foundation

- Non-profit foundation organized to build a next generation IDS/IPS engine
  - Pay developers
  - Organize Suricon
  - Financed by consortium members
    - Big companies (Amazon, …)
    - Startups (Stamus Networks, …)
    - Governmental organizations (ANSSI, …)
- Events:
  - Suricon: Yearly user conference
  - Online Webinars about Suricata
  - Trainings

No network needs Zeek unless proven otherwise

- NO need to run Zeek AND Suricata
  - Zeek and Suricata are NSM
- Save the Earth
  - Don’t run 2 analyzers
  - Unless you monitor ICS
- Save time
  - Think about a new source once you have reached the limits

Objectives of the talk

You should not pass

STAMUS NETWORKS

NO need to run Zeek AND Suricata

Code of conduct compliant objectives

- Show what can be gathered passively on network
  - Using Suricata NSM data
- Demonstrate how IDS and NSM complement each other
  - To provide detection of lateral movement in Windows environment

Tools and data used

Producing and eating JSON together

STAMUS NETWORKS

SELKS

- **S**uricata
- **E**lasticsearch
- **L**ogstash
- **K**ibana
- **S**tamus Community Edition

Also including:
- Arkime
- EveBox
- CyberChef

Source: Stamus Networks

Jupyter notebook

- Open Source platform that uses IPython to provide an interactive data science interface
- We will use it together with some Python code to play around with the data provided by Suricata
- Supports Aggregation, Filtering and different visualizations like a plot
- Often associated with pandas

Malware Traffic Analysis

- PCAP files of attack and malware
  - Mostly in windows environment
- Updated frequently with new samples
- URL: https://www.malware-traffic-analysis.net/

Windows environment

Because, life, you know

STAMUS NETWORKS

Windows environment in Suricata

- Support for main protocols
  - SMB
  - Kerberos
  - DCERPC
  - Flow
- Associated protocols
  - DNS
  - DHCP
- Missing
  - LDAP
  - Decryption of protocols

Building Surface Attack in Jupyter notebook

Well, because AI is the future of mankind

STAMUS NETWORKS

Suricata Analytics

Suricata Analytics is a Jupyter based system

- Connect to SELKS
  - Use REST API
  - Get data from Elasticsearch
- Contains
  - Sample notebook
  - Research notebook
- Github: https://github.com/StamusNetworks/suricata-analytics

Flow log

- dedicated “flow_id” for each flow
- network metadata
- details about the packets/bytes and state
- If an alert was triggered by a signature “alerted” would be true
- Additional protocol details like flags as seen for TCP for example


```
"timestamp": "2013-06-19T02:25:23.331695+0200",
"flow_id": 2014073692127581,
"event_type": "flow",
"src_ip": "172.16.101.196",
"src_port": 49427,
"dest_ip": "192.186.248.36",
"dest_port": 80,
"proto": "TCP",
"app_proto": "http",
"flow": {
  "pkts_toserver": 103,
  "pkts_toclient": 165,
  "bytes_toserver": 12608,
  "bytes_toclient": 216301,
  "start": "2015-03-03T20:09:11.010186+0100",
  "end": "2015-03-03T20:09:28.302533+0100",
  "age": 17,
  "state": "closed",
  "reason": "timeout",
  "alerted": false
},
"tcp": {
  "tcp_flags": "1b",
  "tcp_flags_ts": "1b",
  "tcp_flags_tc": "1b",
  "syn": true,
  "fin": true,
  "psh": true,
  "ack": true,
  "state": "closed",
  "ts_max_regions": 1,
  "tc_max_regions": 1
}
```

Find internal servers: code

[5]:
```
builder = ESQueryBuilder()
builder.set_index('logstash-flow-*')
builder.set_page_size(0)
builder.set_from_date(global_from_date)
builder.set_to_date(global_to_date)

qfilter = 'event_type: flow AND flow.pkts_toclient:[1 TO *] AND (dest_ip:"10.0.0.0/8" OR dest_ip:"172.16.0.0/12" OR dest_ip:"192.168.0.0/16")'
builder.set_qfilter(qfilter)

builder.add_aggs('dest_ip.keyword', order='_count', sort='desc', size=10)
builder.add_aggs('proto.keyword', order='_count', sort='desc', size=10)
builder.add_aggs('dest_port', order='_count', sort='desc', size=10)
builder.add_aggs('app_proto.keyword', order='_count', sort='desc', size=10)
builder.add_aggs('src_ip.keyword', order='_count', sort='desc', size=10)

r = builder.post()
content = r.json()

keys = ['Server', 'Proto', 'Port', 'App', 'Client', 'Count']
res = flatten_aggregation(content, keys)

df = res.groupby(['Server', 'Proto', 'Port', 'App']).agg({'Client': ','.join, 'Count': 'sum'})
df
```

Find internal servers: output

5]:

Server	Proto	Port	App	Client	Count
10.6.15.187	TCP	445	smb	10.6.15.119	2
10.6.15.5	TCP	88	krb5	10.6.15.119,10.6.15.187,10.6.15.93	142
		135	dcerpc	10.6.15.119,10.6.15.187,10.6.15.93	158
		389	failed	10.6.15.187,10.6.15.119,10.6.15.93	170
		445	smb	10.6.15.119,10.6.15.187,10.6.15.93	94
		49674	dcerpc	10.6.15.119,10.6.15.187,10.6.15.93	158
	UDP	53	dns	10.6.15.119,10.6.15.187,10.6.15.93	1010
		123	ntp	10.6.15.119,10.6.15.187,10.6.15.93	66
		389	failed	10.6.15.187,10.6.15.119,10.6.15.93	126
10.6.15.93	TCP	445	smb	10.6.15.119	2

DNS format

- “flow_id” to correlate events of a flow
- DNS protocol details, depending on the query/response
  - complete chain can be tracked

DNS SRV request/response

- SRV request is used by client
  - To find service for a protocol
  - Record set up by Active Directory
  - Most common request is ldap
- Interest
  - Identify the infrastructure
    - Answer will give info on infrastructure
  - Rogue devices
    - Asking for a different domains

SRV requests: code

```
']:
# Get services + clients
builder = ESQueryBuilder()
builder.set_index('logstash-dns-*')
builder.set_page_size(0)

# HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
#qfilter = 'event_type: tls AND (NOT (tls.version.keyword:"TLS 1.2" OR tls.version.keywo
qfilter='event_type:dns AND dns.type:query AND dns.rrtype:SRV'

builder.set_qfilter(qfilter)

builder.add_aggs('dns.rrname.keyword', order='_count', sort='desc', size=10)
builder.add_aggs('src_ip.keyword', order='_count', sort='desc', size=10)

builder.set_from_date(global_from_date)
builder.set_to_date(global_to_date)

r = builder.post()
content = r.json()

keys = ['Request', 'Client', 'Count']
res = flatten_aggregation(content, keys)

df = res.sort_values('Count', ascending=False)
df
```

SRV request: output

```
df
```

[47]:

	Request	Client	Count
0	_ldap._tcp.Default-First-Site-Name._sites.Phantasmedia-DC.phantasmedia.com	10.7.5.101	3
1	_ldap._tcp.Phantasmedia-DC.phantasmedia.com	10.7.5.101	3
2	_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.phantasmedia.com	10.7.5.101	1
3	_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.phantasmedia.com	10.7.5.101	1
4	_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.phantasmedia.com	10.7.5.101	1
5	_ldap._tcp.Default-First-Site-Name._sites.gc._msdcs.phantasmedia.com	10.7.5.101	1
6	_ldap._tcp.Default-First-Site-Name._sites.phantasmedia.com	10.7.5.101	1
7	_ldap._tcp.pdc._msdcs.phantasmedia.com	10.7.5.101	1

Find the users

Everything starts from a user

STAMUS NETWORKS

SMB NTLMSSP format

- Ntlmssp contains
  - User
  - Domain
  - Host
  - Version
- Easy usage to find auth users


```
{
  "timestamp": "2021-06-16T19:14:48.326949+0200",
  "flow_id": 1562112648859374,
  "pcap_cnt": 646986,
  "event_type": "smb",
  "src_ip": "10.6.15.119",
  "src_port": 65102,
  "dest_ip": "10.6.15.5",
  "dest_port": 445,
  "proto": "TCP",
  "smb": {
    "id": 4,
    "dialect": "3.11",
    "command": "SMB2_COMMAND_SESSION_SETUP",
    "status": "STATUS_SUCCESS",
    "status_code": "0×0",
    "session_id": 228698687012957,
    "tree_id": 0,
    "ntlmssp": {
      "domain": "SALTMOBSTERS",
      "user": "tommy.vega",
      "host": "DESKTOP-NIEE9LP",
      "version": "10.0 build 19041 rev 15"
    }
  }
}
```

Kerberos format

- “flow_id” to correlate events of a flow
- Protocol specific commands
- Contains
  - User name in sname
  - Domain in realm
  - Other technical info


```
"timestamp": "2019-02-20T23:02:23.886317+0100",
"flow_id": 2105186308043491,
"pcap_cnt": 6619717,
"event_type": "krb5",
"src_ip": "10.2.20.101",
"src_port": 49182,
"dest_ip": "10.2.20.2",
"dest_port": 88,
"proto": "TCP",
"pkt_src": "wire/pcap",
"krb5": {
  "msg_type": "KRB_TGS_REP",
  "cname": "RHODES-WIN-PC$",
  "realm": "PELICANWORKS.INFO",
  "sname": "rhodes-win-pc$",
  "encryption": "aes256-cts-hmac-sha1-96",
  "weak_encryption": false,
  "ticket_encryption": "aes256-cts-hmac-sha1-96",
  "ticket_weak_encryption": false
}
```

Detecting user anomaly

- Remotely list users “connected” on a system
  - Usually systems have a single user
  - Or really few
- Find systems with a lot of users
  - Citrix/TSE servers
  - Owned systems
    - User scan
- Find systems with high privilege user
  - Regular ?
  - Privilege escalation ?

File analysis

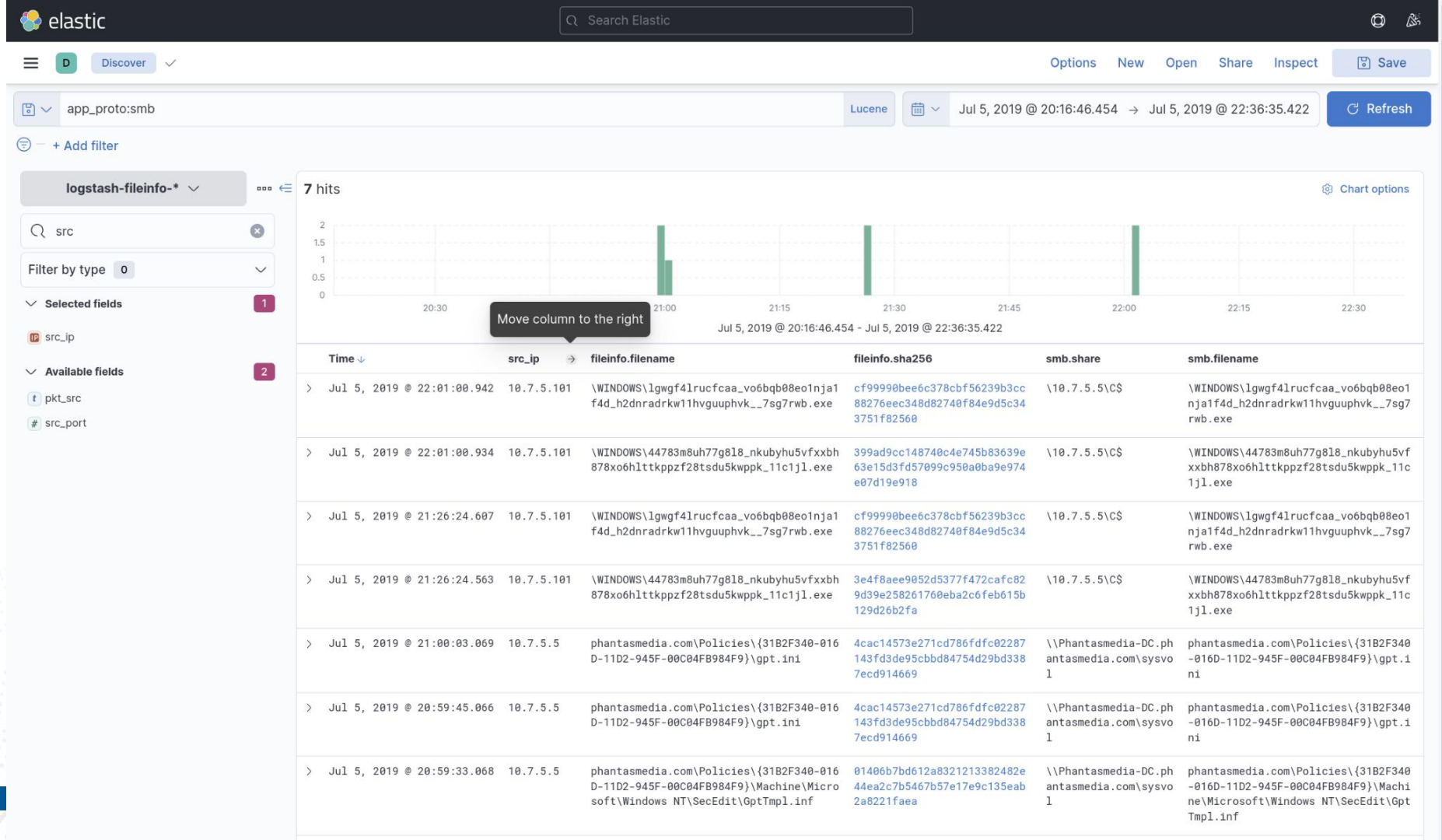
Over SMB or else

STAMUS NETWORKS

File Format

- “flow_id” to correlate events of a flow
- Protocol metadata where file transfer was seen
- Request details
- File details
  - Filename and Checksum
  - Filetype
  - Files can also be stored if configured


```
{
  "timestamp": "2019-07-05T22:01:56.397716+0200",
  "flow_id": 1433289318713385,
  "pcap_cnt": 34955,
  "event_type": "fileinfo",
  "src_ip": "5.188.168.49",
  "src_port": 80,
  "dest_ip": "10.7.5.101",
  "dest_port": 49997,
  "proto": "TCP",
  "http": {
    "hostname": "5.188.168.49",
    "url": "/win.png",
    "http_content_type": "image/png",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 113638
  },
  "app_proto": "http",
  "fileinfo": {
    "filename": "/win.png",
    "sid": [],
    "magic": "PE32 executable (GUI) Intel 80386, for MS Windows, 4 sections",
    "gaps": false,
    "state": "TRUNCATED",
    "sha256": "279364751013303a40cc19426b364272cf0ace82e0039c356e27b4949b9bdc55",
    "stored": false,
    "size": 102400,
    "tx_id": 0
  }
}
```


elastic
Search Elastic
D
Discover
Options
New
Open
Share
Inspect
Save
app_proto:smb
Lucene
Jul 5, 2019 @ 20:16:46.454 → Jul 5, 2019 @ 22:36:35.422
Refresh
+ Add filter
logstash-fileinfo-*
src
Filter by type 0
Selected fields 1
src_ip
Available fields 2
pkt_src
src_port
7 hits
Chart options
2
1.5
1
0.5
0
20:30
21:00
21:15
21:30
21:45
22:00
22:15
22:30
Move column to the right
Jul 5, 2019 @ 20:16:46.454 - Jul 5, 2019 @ 22:36:35.422
Time
src_ip
fileinfo.filename
fileinfo.sha256
smb.share
smb.filename
Jul 5, 2019 @ 22:01:00.942
10.7.5.101
\WINDOWS\lgwgf4lrucfcaa_vo6bqb08eo1nja1f4d_h2dnradrkw11hvguuphvk__7sg7rwb.exe
cf99990bee6c378cbf56239b3cc88276eec348d82740f84e9d5c343751f82560
\10.7.5.5\C$
\WINDOWS\lgwgf4lrucfcaa_vo6bqb08eo1nja1f4d_h2dnradrkw11hvguuphvk__7sg7rwb.exe
Jul 5, 2019 @ 22:01:00.934
10.7.5.101
\WINDOWS\44783m8uh77g8l8_nkubyhu5vfxxbh878xo6hlttkppzf28tsdu5kwppk_11c1jl.exe
399ad9cc148740c4e745b83639e63e15d3fd57099c950a0ba9e974e07d19e918
\10.7.5.5\C$
\WINDOWS\44783m8uh77g8l8_nkubyhu5vfxxbh878xo6hlttkppzf28tsdu5kwppk_11c1jl.exe
Jul 5, 2019 @ 21:26:24.607
10.7.5.101
\WINDOWS\lgwgf4lrucfcaa_vo6bqb08eo1nja1f4d_h2dnradrkw11hvguuphvk__7sg7rwb.exe
cf99990bee6c378cbf56239b3cc88276eec348d82740f84e9d5c343751f82560
\10.7.5.5\C$
\WINDOWS\lgwgf4lrucfcaa_vo6bqb08eo1nja1f4d_h2dnradrkw11hvguuphvk__7sg7rwb.exe
Jul 5, 2019 @ 21:26:24.563
10.7.5.101
\WINDOWS\44783m8uh77g8l8_nkubyhu5vfxxbh878xo6hlttkppzf28tsdu5kwppk_11c1jl.exe
3e4f8aee9052d5377f472cafc829d39e258261760eba2c6feb615b129d26b2fa
\10.7.5.5\C$
\WINDOWS\44783m8uh77g8l8_nkubyhu5vfxxbh878xo6hlttkppzf28tsdu5kwppk_11c1jl.exe
Jul 5, 2019 @ 21:00:03.069
10.7.5.5
phantasmedia.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
4cac14573e271cd786fdfc02287143fd3de95cbbd84754d29bd3387ecd914669
\\Phantasmedia-DC.phantasmedia.com\sysvol
phantasmedia.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
Jul 5, 2019 @ 20:59:45.066
10.7.5.5
phantasmedia.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
4cac14573e271cd786fdfc02287143fd3de95cbbd84754d29bd3387ecd914669
\\Phantasmedia-DC.phantasmedia.com\sysvol
phantasmedia.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\gpt.ini
Jul 5, 2019 @ 20:59:33.068
10.7.5.5
phantasmedia.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
01406b7bd612a8321213382482e44ea2c7b5467b57e17e9c135eab2a8221faea
\\Phantasmedia-DC.phantasmedia.com\sysvol
phantasmedia.com\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf

What is wrong there ?

- Desktop sending an executable exe:
  - To Windows directory
  - On Active Directory server
- High entropy on filename
- Usage of IP addresses and not hostname

Stamus Lateral ruleset

Find notable events in SMB/DCERPC traffic

STAMUS NETWORKS

Stamus Lateral ruleset

- Detection of non standard behavior
  - Remote low level administration action
  - Never used by users
- Examples:
  - Remote creation of a net share
  - Remote creation of scheduled tasks
  - Remote creation of a service
  - Remote installation of a printer driver
  - DC enumeration

Availability

- License: GPLv3
- Info and download: https://www.stamus-networks.com/blog/new-open-ruleset-for-detecting-lateral-movement-with-suricata

A lot of activity

	Timestamp	Signature	Source IP	Destination IP	Proto	Probe	Category	Tag
–	2019-07-05, 10:01:04 pm	SN MS-SCMR service - ROpenSCManagerW	10.7.5.101	10.7.5.5	smb	2019-07-05-Ursnif-with-Trickbot-and-IcedID.pcap		untagged

Synthetic view | Related Alerts 20 | Related Anomaly 1 | Related File Info 2 | Related SMB 77 | JSON View | PCAP File

	Timestamp	Signature	SignatureID	Category	Mitre Tactic	Mitre Technique
+	2019-07-05 22:01:04	SN MS-SCMR service - RCloseServiceHandle	3115470		n/a	n/a
+	2019-07-05 22:01:04	SN MS-SCMR service - RDeleteService	3115472		n/a	n/a
+	2019-07-05 22:01:04	SN MS-SCMR service - RCloseServiceHandle	3115470		n/a	n/a
+	2019-07-05 22:01:04	SN MS-SCMR service - ROpenSCManagerW	3115482		n/a	n/a
+	2019-07-05 22:01:04	SN MS-SCMR service - ROpenServiceW	3115483		n/a	n/a
+	2019-07-05 22:01:01	SN MS-SCMR service - RCloseServiceHandle	3115470		n/a	n/a
+	2019-07-05 22:01:01	SN MS-SCMR service - RCloseServiceHandle	3115470		n/a	n/a
+	2019-07-05 22:01:00	SN MS-SCMR service - RStartServiceW	3115111		n/a	n/a
+	2019-07-05 22:01:00	SN MS-SCMR service - ROpenServiceW	3115483		n/a	n/a
+	2019-07-05 22:01:00	SN MS-SCMR service - RCreateServiceW	3115102		n/a	n/a

< 1 2 >

STAMUS NETWORKS

SMB events on same flow

	Timestamp	Signature	Source IP	Destination IP	Proto	Probe	Category	Tag
−	2019-07-05, 10:01:04 pm	SN MS-SCMR service - RCloseServiceHandle	10.7.5.101	10.7.5.5	smb	2019-07-05-Ursnif-with-Trickbot-and-IcedID.pcap		untagged

Synthetic view | Related Alerts 20 | Related Anomaly 1 | Related File Info 2 | Related SMB 77 | JSON View | PCAP File

	Timestamp	Command	Severity	Interface	Endpoint	Uuid	Opnum	Status	Share	Filename	Host	User
+	2019-07-05 22:01:00	SMB1_COMMAND_TREE_CONNECT_ANDX						STATUS_SUCCESS				
+	2019-07-05 22:01:00	SMB1_COMMAND_NT_CREATE_ANDX						STATUS_SUCCESS		\svcctl		
+	2019-07-05 22:01:00	SMB1_COMMAND_WRITE_ANDX						STATUS_SUCCESS				
+	2019-07-05 22:01:00	SMB1_COMMAND_WRITE_ANDX					15	STATUS_SUCCESS				
+	2019-07-05 22:01:00	SMB1_COMMAND_WRITE_ANDX							\10.7.5.5\C$	\WINDOWS\lgwgf4lrucfcaa_vo6bqb08eo1nja1f4d_h2dnradrkw11hvguuphvk__7sg7rwb.exe		
+	2019-07-05 22:01:00	SMB1_COMMAND_CLOSE						STATUS_SUCCESS				
+	2019-07-05 22:01:00	SMB1_COMMAND_TREE_DISCONNECT						STATUS_SUCCESS				
+	2019-07-05 22:01:00	SMB1_COMMAND_TREE_CONNECT_ANDX						STATUS_SUCCESS	\10.7.5.5\C$			
+	2019-07-05 22:01:00	SMB1_COMMAND_NT_CREATE_ANDX						STATUS_SUCCESS		\WINDOWS\lgwgf4lrucfcaa_vo6bqb08eo1nja1f4d_h2dnradrkw11hvguuphvk__7sg7rwb.exe		
+	2019-07-05 22:01:00	SMB1_COMMAND_WRITE_ANDX							\10.7.5.5\C$	\WINDOWS\44783m8uh77g8l8_nkubyhu5vfxxbh878xo6hlttkppzf28tsdu5kwppk_11c1jl.exe		

< 1 2 3 4 5 ••• 8 > 10 / page

Conclusion

NSM & IDS to the rescue

STAMUS NETWORKS

Take away

- Lateral movement detection
  - By using analysis of protocol of Windows stack
  - And generic events
- There is more than one way to find them
- Build detection on a combination of
  - Signature based detection
    - Direct attack
    - Notable events with for example Stamus lateral ruleset
  - Algorithmic detection
    - Manual analysis
    - Statistical
    - AI based