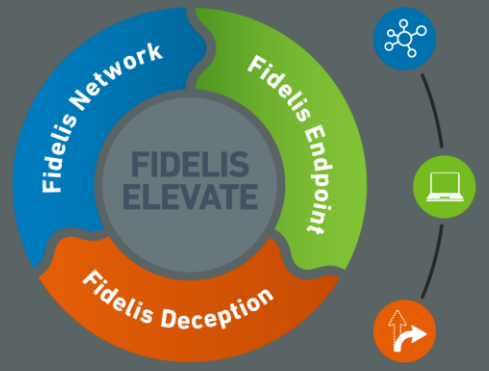
Vizibilita na síti i koncových bodech jako základ pro detekci a analýzu

28. listopadu 2019

ALEXANDER MAŠEK, JAN RYDVAL

Fidelis Cybersecurity



Efektivní vyšetřování a analýza bezpečnostních událostí

Hluboká Vizibilita

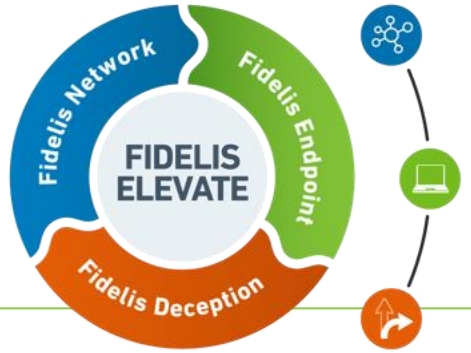
Přesná Detekce Analýza

Rychlá Reakce

Fidelis Elevate – ADR platforma

- **hluboká vizibilitu na dění na síti i koncových bodech**
- **Prevence a detekce | vyšetřování a hunting | reakce a remediace kybernetických incidentů**
- **jednotné uživatelské rozhraní** plně integrovaných modulů :

- **Fidelis Network** – detekce a prevence na síťovém provoz
- **Fidelis Endpoint** – EDR & EPP – ochrana koncových bodů
- **Fidelis Deception** – inteligentní pastičky – proaktivní detekce



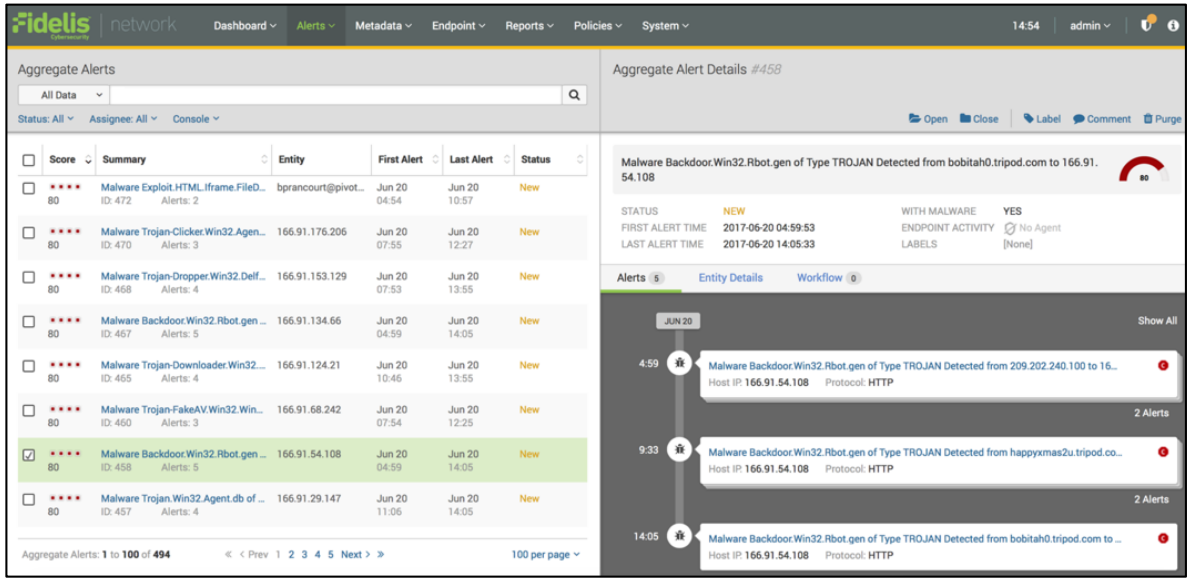
Automatizovaná Detekce a Reakce

Kompletní vizibilita sítě

Hluboká Vizibilita

Rozsah

- **Neselektivně všechny porty & protokoly**
  - Nestandardní & všech 65k portů
  - Popis neznámých protokolů
- **Příchozí & odchozí** komunikace
- Monitoring **v reálném čase i do minulosti**
- Škálovatelné až do 10 Gbps / sensor



Hloubka

- **DPI & DSI** - pakety, spojení & obsah, včetně hluboce ukrytého obsahu
- **Parametry obsahu** (např. import hash, atributy certifikátu)
- **Znalost souvislostí** – parametry popisující způsob přenosu dat
- Možnost doplnit **zákaznická pravidla**

Kompletní vizibilita koncových bodů

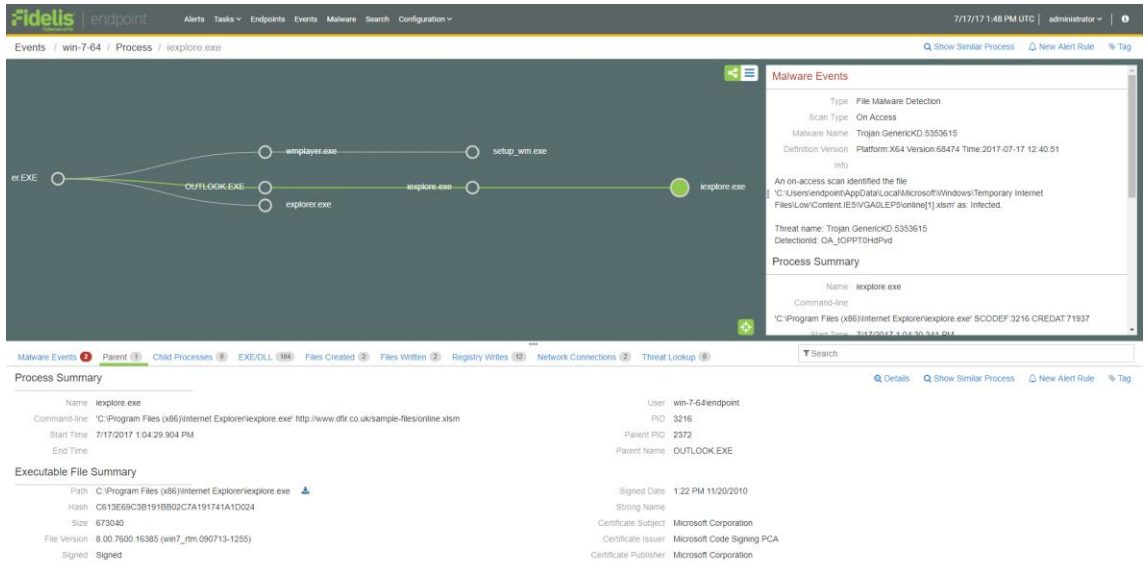
Hluboká Vizibilita

Rozsah

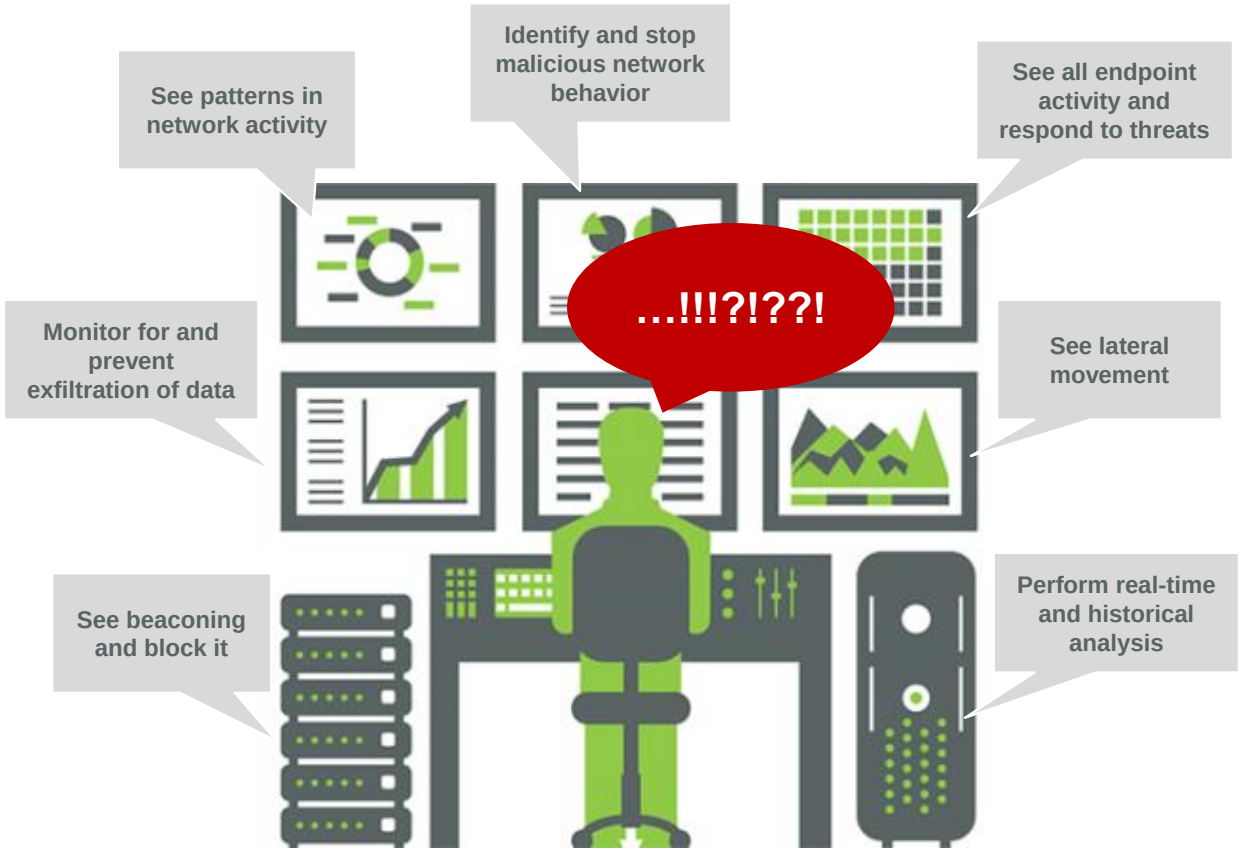
- **Podpora více OS** (MS Windows, Linux, Mac OS)
- Možnost tvorby **vlastních skriptů** a jejich distribuce na koncové body
- **Vyhodnocování zranitelností** na koncových bodech

Hloubka

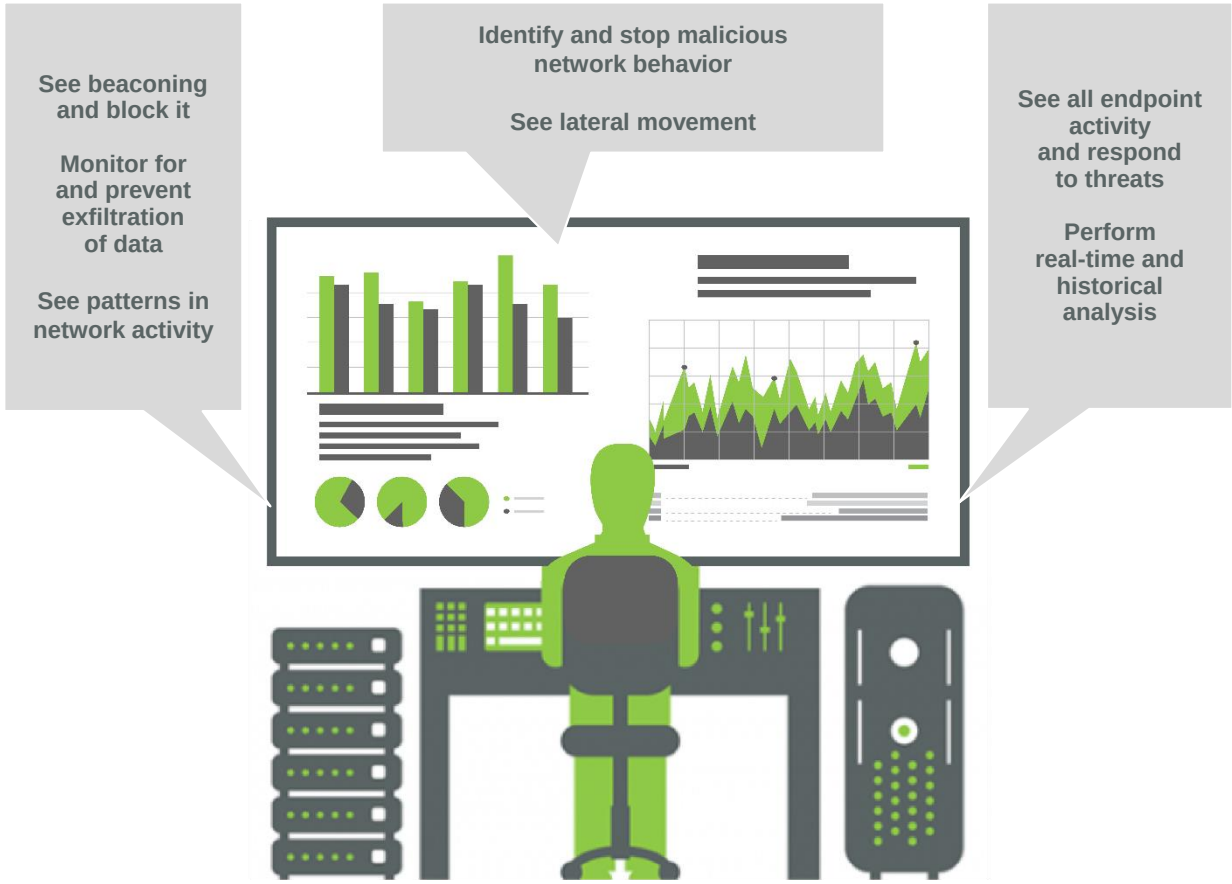
- Spouštění a ukončování **procesů**
- **Souborové** manipulace
- Změny v **registrech**
- Windows Event logy, **DNS** aktivity
- Vystavovaná **síťová spojení**
- Analýza stavu **paměti a OS**
- Systémové a aplikační **zranitelnosti** (např. MS Office)
- **Správa** koncových stanic, rozpoznání nových koncových bodů



Jak zjednodušit a zredukovat vaši bezpečnostní datovou analýzu, setřídit a stanovit priority, vyšetřování a reakce



BEZ NÁS



S FIDELISEM

Malware Alert #187

Export | Layout

Back | 1 of 2 Alerts < Prev | Next > | Find Metadata | New | unassign... | default | 2 | 0 | Purge

Src (Server)	HTTP	Dst (Client)
141.251.2.27 United States [Empty]	80 55098	192.168.2.101 Bratislava, Slovakia [Empty]

Severity: Critical
Threat Score: 80
Alert Time: 2019-03-09 15:27:07
Rule Name: Malware - TROJAN
Conclusion Id: 38 Go to Conclusion
Summary: Malware W32/ObfusInjectBot.a of Type TROJAN Detected from 141.251.2.27 to 192.168.2.101
Labels: demo_network, not_mozilla
Decoding Path: HTTP(mwq.jpg) ↳ binary(FSS_Object...

Additional Information

Filename: FSS_Object-0
Filetype: exe
Filesize: 718 KB
Malware Name: W32/ObfusInjectBot.a

Violation Information

Highlighting ON

Malware Engine: Malware - Static Engine
Rule: Malware - TROJAN
Summary: Malware W32/ObfusInjectBot.a of Type TROJAN Detected from 141.251.2.27 to 192.168.2.101

Related Alerts

Alert Workflow Log

Endpoint Information

No Endpoint Information available for Host IP 192.168.2.101

Malware Information

Malware Name: W32/ObfusInjectBot.a
Malware Type: TROJAN

Sandbox Report

Decoding Path & Channel Attributes

Safe Download OFF

HTTP

Download

Filename: mwq.jpg
Url: 172.16.40.1/virus/mwq.jpg
ContentType: image/jpeg
Command: GET
Status Code: 200
UserAgent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.21 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
Host: 172.16.40.1
Server: nginx/1.13.12
Connection: keep-alive

binary

Download

Filename: FSS_Object-0
Suspicious: Pad (8 bytes)

Recorded Session

Overview | Recorded Client Data | Recorded Server Data

Malware Alert #187

Export | Layout

Back | 1 of 2 Alerts < Prev | Next > | Find Metadata | New | unassign... | default | 2 | 0 | Purge

Src (Server)	HTTP	Dst (Client)
141.251.2.27 United States [Empty]	80 55098	192.168.2.101 Bratislava, Slovakia [Empty]

Severity	Critical
Threat Score	80
Alert Time	2019-03-09 15:27:07
Rule Name	Malware - TROJAN
Conclusion Id	38 Go to Conclusion
Summary	Malware W32/ObfusInjectBot.a of Type TROJAN Detected from 141.251.2.27 to 192.168.2.101
Labels	demo_network, not_mozilla
Decoding Path	HTTP(mwq.jpg) ↳ binary(FSS_Object...

Additional Information

Filename	FSS_Object-0
Filetype	exe
Filesize	718 KB
Malware Name	W32/ObfusInjectBot.a

Sandbox Report

Full Page

Analysis Report (Metadata)

Malware Score	100
ID	119805214
OS	win7
Started	2019-06-06 08:02:26
Ended	2019-06-06 08:06:03
Duration	217 Seconds
File Name	uv.exe
Analyzed As	PE32 executable (GUI) Intel 80386, for MS Windows, RAR self-extracting archive
SHA256	c34d903ef5c004b86a82fdf0f6ac3016ae612e4e419b62ac42b3a907e4f52cbe
SHA1	ed5bc8cb6d13b05a669d52b88c2cd33855c29570
MD5	29ad18b86f1620890b37ff4fd537edae

Behavior Indicators

FSS_SBA_Feeds	Score: 25
FSS_SBA_Classifier	Score: 151
FS_Startup_Roaming	Score: 40

Forensic Data

Text | Hex

```
4d 5a 90 00 03 00 00 00   04 00 00 00 ff ff 00 00    M
b8 00 00 00 00 00 00 00   40 00 00 00 00 00 00 00    Z.....@.....
00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    ....
00 00 00 00 00 00 00 00   00 00 00 00 e0 00 00 00    @.....
0e 1f ba 0e 00 b4 09 cd   21 b8 01 4c cd 21 54 68    ....!..L.!Thi
69 73 20 70 72 6f 67 72   61 6d 20 63 61 6e 6e 6f    s.program.cannot.b
74 20 62 65 20 72 75 6e   20 69 6e 20 44 4f 53 20    e.run.in.DOS.mod
6d 6f 64 65 2e 0d 0d 0a   24 00 00 00 00 00 00 00    e....$.....[...
5b da c1 ae 1f bb af fd   1f bb af fd 1f bb af fd    .....
16 c3 3a fd 04 bb af fd   16 c3 2c fd 9f bb af fd    .....:.....,.....
16 c3 3c fd 0a bb af fd   1f bb ae fd f2 bb af fd    ..<.....+.
16 c3 2b fd 7b bb af fd   16 c3 3d fd 1e bb af fd    {.....=.....;.
16 c3 3b fd 1e bb af fd   16 c3 3e fd 1e bb af fd    .....>....Rich
52 69 63 68 1f bb af fd   00 00 00 00 00 00 00 00    ..........PE..
50 45 00 00 4c 01 04 00   82 0b 16 52 00 00 00 00    L.....
00 00 00 00 e0 00 03 01   0b 01 09 00 00 52 02 00    R.....
00 9a 00 00 00 00 00 00   48 d3 01 00 00 10 00 00    R.....
00 70 02 00 00 00 40 00   00 10 00 00 00 02 00 00    H.....p....
05 00 00 00 00 00 00 00   05 00 00 00 00 00 00 00    @.....
00 20 05 00 00 04 00 00   00 00 00 00 02 00 00 81    .....
00 00 10 00 00 10 00 00   00 00 10 00 00 10 00 00    .....
00 00 00 00 10 00 00 00   10 bf 02 00 33 00 00 00    .....3...
6c ab 02 00 dc 00 00 00   00 e0 04 00 dc 35 00 00    l.....5.....
00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    .....
00 00 00 00 00 00 00 00   f0 73 02 00 1c 00 00 00    ...s..
00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    .....
00 00 00 00 00 00 00 00   80 9b 02 00 40 00 00 00    .....
00 00 00 00 00 00 00 00   00 70 02 00 74 03 00 00    .....p..
00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00    @.....
00 00 00 00 00 00 00 00   2e 74 65 78 74 00 00 00    t.....text...~
7e 51 02 00 00 10 00 00   00 52 02 00 00 04 00 00    .....
00 00 00 00 00 00 00 00   00 00 00 00 20 00 00 60    Q.....
```

Malware Alert #1201

Export Layout

Back 2 of 3 Alerts < Prev | Next > Find Metadata New unassign... default 1 2 Purge

Src (Server)	HTTP	Dst (Client)
23.229.156.226 United States www.sharks...	80 49923	192.168.200.90 Prague, Czech Republic WINDOWS1...

Severity Critical
Threat Score 90
Alert Time 2019-04-03 09:26:21
Rule Name Malware - TROJAN
Conclusion Id 157 Go to Conclusion
Summary Malware GenericRXFZ-QD!3490B382D4DB of Type TROJAN Detected from www.sharkswithlaserbeams.biz to 192.168.200.90
Labels demo_endpoint
Decoding Path HTTP(Demo-Ransom...
↳ chunked(Demo-R...
↳ gzip(Demo-Rans...

Additional Information

Filename Demo-Ransomware.exe
Filetype exe
Filesize 230 KB
Malware Name GenericRXFZ-

Endpoint Information

Endpoint Tasks

Logged in User *[Empty]*
Agent ID bbf02f4d-8d6f-40ed-8a5d-aa0a051efee9

Validation 4 | Enrichment 3 | Detections 2 | Endpoint Tasks 2

Endpoint Activity Detected
Rule information not available

Event 3: Process Start (More Details) < Prev 3 of 4 Next >

Process Summary

Name installer.exe
Command-line C:\Temp\installer.exe
Start Time 2019-04-03 9:26:32
User WINDOWS10CLIENT\fidelis
PID 5852

Executable File Summary

Path C:\Temp\installer.exe
Hash 3490b382d4dbdc1a8ae9f1957c3a3867
Size 230 KB
File Version 2.0.0.0

Decoding Path & Channel Attributes

Safe Download OFF

DNSResolution

Server FQDN www.sharkswithlaserbeams.biz
Server CNAME sharkswithlaserbeams.biz

HTTP

Download

Filename Demo-Ransomware.exe
Url www.sharkswithlaserbeams.biz/Demo-Ransomware.exe
ContentType application/x-msdownload
Command GET
Status Code 200
UserAgent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)
Host www.sharkswithlaserbeams.biz
Connection Keep-Alive
Server Apache
Connection Upgrade, Keep-Alive

↳ chunked

Download

Filename Demo-Ransomware.exe

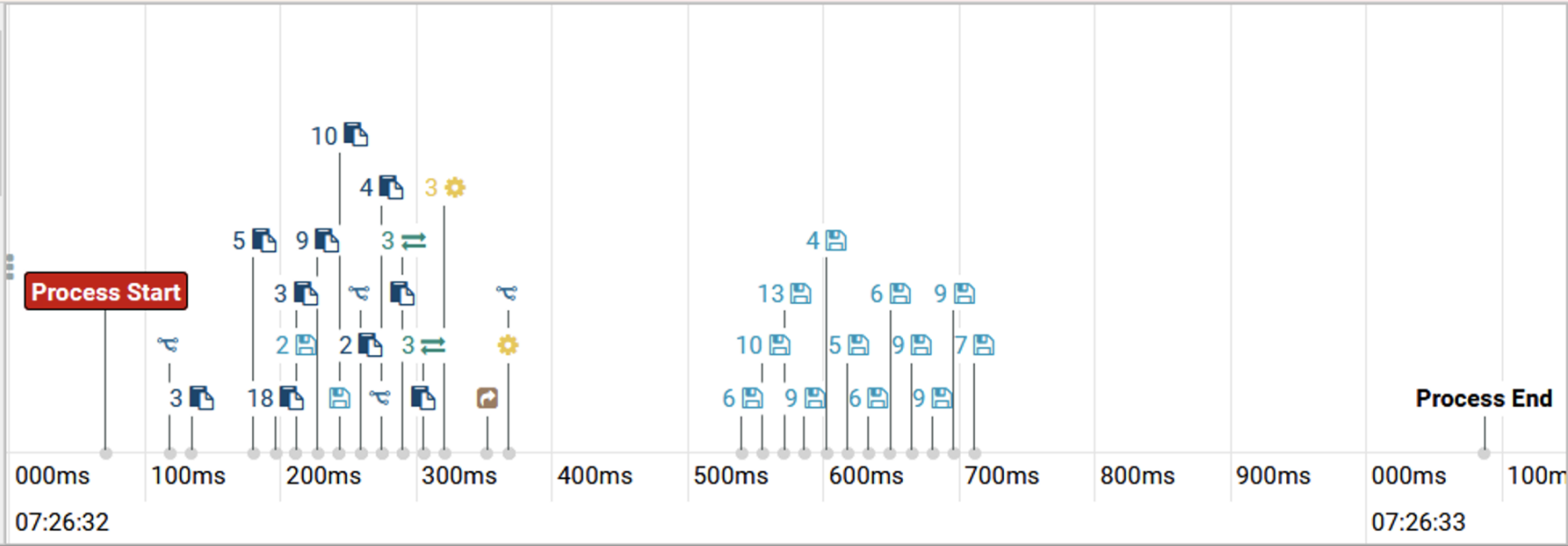
↳ gzip

Download

Filename Demo-Ransomware.exe

Process Summary

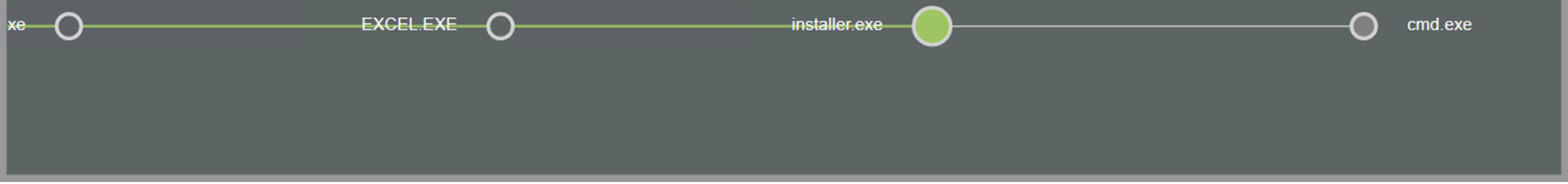
Endpoint	Windows10ClientA
Name	installer.exe
Command-line	C:\Temp\installer.exe
Start Time	2019/04/03 07:26:32.071
End Time	2019/04/03 07:26:33.087
User	WINDOWS10CLIENT\fidelis
PID	5852
Parent PID	5260
Parent Name	EXCEL.EXE



Search

Submit

Alerts | Parent | Process Tree | Child Processes | Remote Threads | EXE/DLL | Files Created | Files Written | Files Closed | Registry Writes | Network Connections

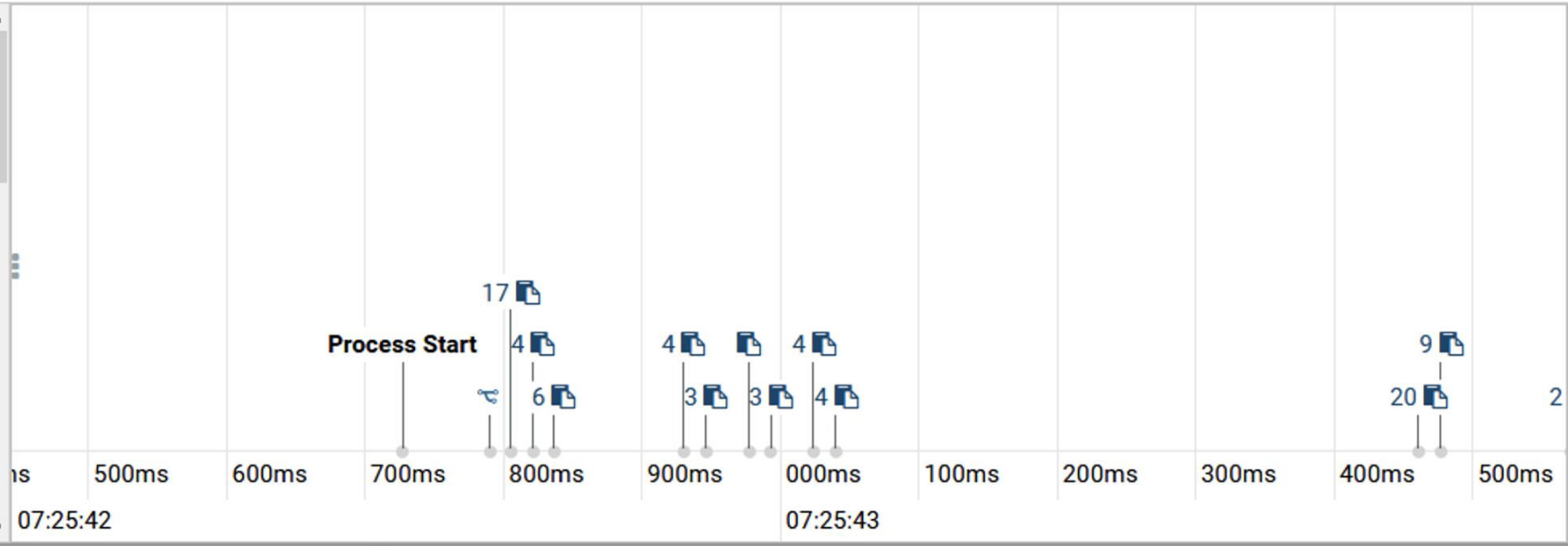


Windows10ClientA / Process / firefox.exe

New Behavior Rule | Create Yara Rule | Reports | Tag | Start Task

Process Summary

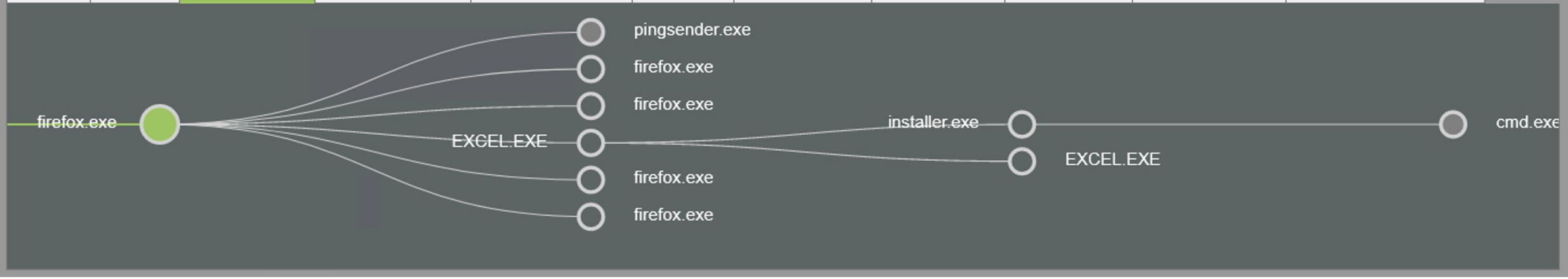
Endpoint Windows10ClientA
Name firefox.exe
Command-line "C:\Program Files (x86)\Mozilla Firefox\firefox.exe"
Start Time 2019/04/03 07:25:42.727
End Time 2019/04/03 07:26:48.086
User WINDOWS10CLIENT\fidelis
PID 4396
Parent PID 4932
Parent Name updater.exe



Search

Submit

Alerts | Parent | Process Tree | Child Processes | Remote Threads | EXE/DLL | Files Created | Files Written | Files Closed | Registry Writes | Network Connections



Metadata… základ pro analýzu!

Hluboká Vizibilita

Přesná Detekce Analýza

KDO:

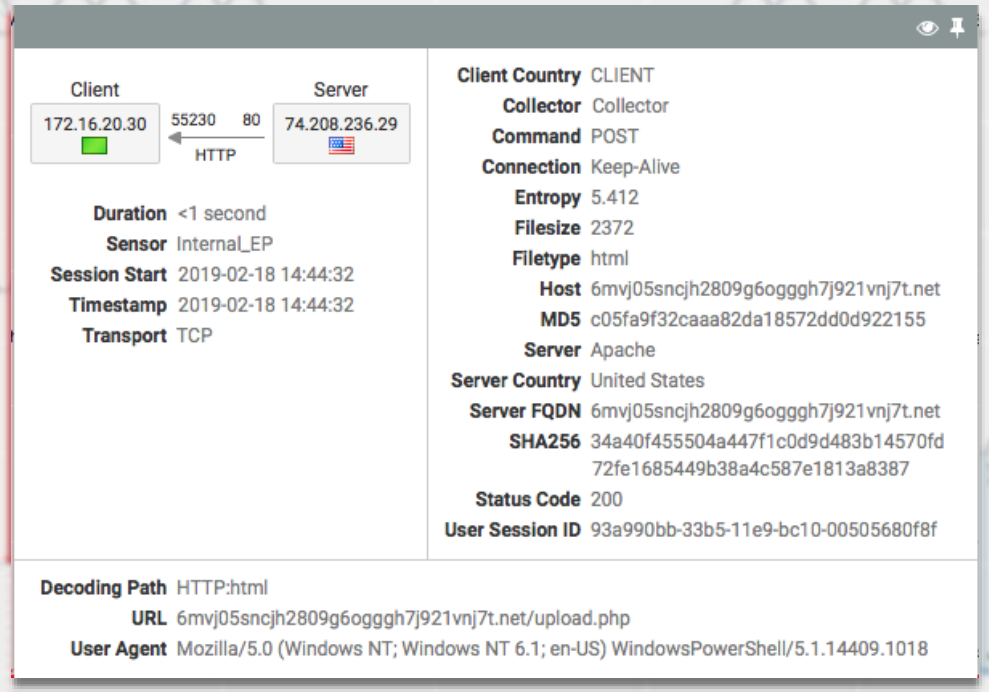
Doménový uživatel, Webmail uživatel, FTP uživatel, emailová adresa, device ID, organizace

CO:

Název souboru, SHA256, MD5, tagování obsahu, jméno a typ malware

KDY:

Od současnosti zpět do historie až do dobu, po jakou jste ochotni ukládat metadata



KDE:

Zdroj, destinace, geolokace/země, IP adresa, organizace, URL, doména

JAK:

protokoly, aplikace, typy souborů, User Agent, zákaznické protokoly, zamaskované a vnořené soubory a skripty

Ruční vyhledávání, automatické analýzy, detekce anomálií…
Za zlomek nákladů tzv. PCAP systému a s mnohem rychlejší odezvou.

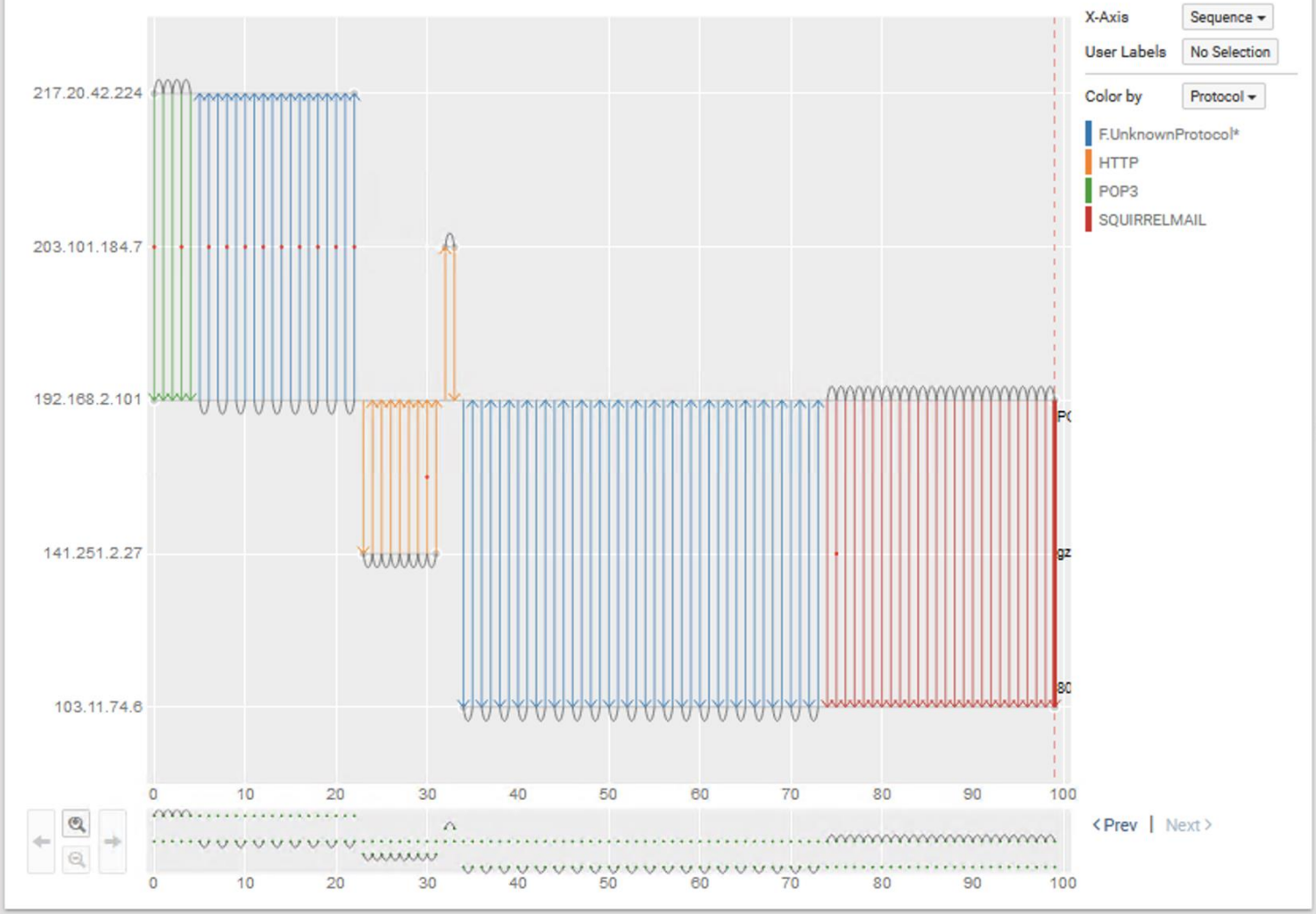
Default Filter *

Actions | Layout

Time Range | Advanced | Sensor = Direct | Client IP = 192.168.2.101 | Protocol != TLS | Clear All

Time: Mar 09, 15:03:12 - Mar 09, 15:58:12 | Transactions: 1 to 100 of 100 | 100 per page | Sorting: Time Des | Previous 1 Next | Collector: Collector

Graphical View



Metadata Details

Sensor: Direct **Session:** 6666397808009867027 **Session Size:** 0 Bytes, 0 Packets **Related Alerts:** 1

Client	SQUIRRELMAIL	Server
192.168.2.101 Slovakia	37944 80	103.11.74.6 Indonesia

Decoding Paths

- HTTP(compose.php)
  - attributes
    - Filename = compose.php
    - URL = webmail.pilferdata.com/src/compose.php
    - ContentType = multipart/form-data; boundary=----WebKitFormBoundaryAezAdMTWAmASbsEL
    - Command = POST
    - StatusCode = 200
    - Host = webmail.pilferdata.com
    - Connection = keep-alive
    - UserAgent = Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.1
    - Referer = http://webmail.pilferdata.com/src/compose.php?mailbox=INBOX&startMessage=1
    - Server = Apache
    - Connection = Keep-Alive
  - SQUIRRELMAIL(cc_name.9.tgz)
    - attributes
      - Filename = cc_name.9.tgz
      - Mode = Upload file
      - AppUser = nickcopeland@pilferdata.com
      - From = nickcopeland@pilferdata.com
    - gzip(cc_name.9.tar)
      - attributes
        - Filename = cc_name.9.tar
        - Filename = cc_name.8.tar
        - Filename = cc_name.7.tar
        - Filename = cc_name.6.tar
        - Filename = cc_name.5.tar
        - Filename = cc_name.4.tar
        - Filename = cc_name.3.tar
        - Filename = cc_name.2.tar

DSI Alert #217

Export | Tune | Layout

Back | Find Metadata | New | unassign... | default | 1 | 0 | Purge

Conclusion Id 43 Go to Conclusion

Summary CreditCard number(s) going from 192.168.2.101 to 103.11.74.6 over protocol SQUIRRELMAIL

Labels demo_network

Decoding Path HTTP(compose.php)
↳ SQUIRRELMAIL(cc_name.9.tgz)
↳ gzip(cc_name.9.tar)
↳ tar(cc_name.8.tgz)
↳ gzip(cc_name.8.tar)
↳ tar(cc_name.7.tgz)
↳ gzip(cc_name.7.tar)
↳ tar(cc_name.6.tgz)
↳ gzip(cc_name.6.tar)
↳ tar(cc_name.5.tgz)
↳ gzip(cc_name.5.tar)
↳ tar(cc_name.4.tgz)
↳ gzip(cc_name.4.tar)
↳ tar(cc_name.3.tgz)
↳ gzip(cc_name.3.tar)
↳ tar(cc_name.2.tgz)
↳ gzip(cc_name.2.tar)
↳ tar(cc_name.1.tgz)
↳ gzip(cc_name.1.tar)
↳ tar(cc_name.0.tgz)
↳ gzip(cc_name.0.tar)
↳ tar(cc_name.zip)
↳ zip(cc_name.0pad)
↳ binary(FSS_Object-0)
↳ zip(cc_name.xor)
↳ binary(FSS_Object-0)

Additional Information

Filename FSS_Object-0

Filetype oasis-document

Violation Information

Highlighting ON

Rule JR_CreditCard Number

Summary CreditCard number(s) going from 192.168.2.101 to 103.11.74.6 over protocol SQUIRRELMAIL

Matched On

JR.CreditCard_Number

Match on

CreditCard

Decoding Path & Channel Attributes

Safe Download OFF

oasis-document

Creation Date Fri Jul 11 17:27:22 2014 UTC

Modification Date Fri Jul 11 17:28:20 2014 UTC

HTTP

Download

Filename compose.php

Url webmail.pilferdata.com/src/compose.php

ContentType multipart/form-data; boundary=----WebKitFormBoundaryAezAdMTWAmASbsEL

Command POST

Host webmail.pilferdata.com

Connection keep-alive

UserAgent Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.114 Safari

Recorded Session

Forensic Data

Text | Hex

Adam Abbott 5443-6127-6701-3598 11/13/1961
Brent Carter 4658-1655-4892-4743 10/04/1935
Charles Bullock 3339-5231-7456-9209 01/30/1943
Dean Deacon 3707-915930-48412 06/01/1938
Emily Elwood 4687-9961-7724-8763 11/24/1945
Francis Fergusson 4821-90999-1510 02/20/1974
Gilly Garnett 5101-3820-8221-1227 12/23/1934
Heather Hallewell 4612-1943-2272-2961 07/11/1993
Ian Inglefield 5321-6977-1177-4103 03/10/1942
Jerry Jackson 3710-687013-91326 10/08/1965
Katie Kapoor 4167-6977-2379-3943 06/12/1922
Leslie Lancaster 4487-1930-5475-6223 08/19/1958
Michael MacGreggor 5146-0309-0405-4898 05/18/2002
Leslie Lockwood 5480-4328-2234-3383 04/22/1954
Norbert Nicholls 4272-1023-6756-9099 09/15/1914
Oliver Ogrady 4389-2266-4889-6672 08/10/1951
Peter Patterson 5206-4214-1360-2201 10/26/1956
John Quinn 3442-763729-93320 09/24/1981
Rowan Rathbone 3432-359223-98860 04/11/1965
Simon Schofield 4194-6589-7158-3714 06/07/1962
Toby Thurman 4539-6783-3513-3406 02/07/1974
Urwin Underwood 6011-3887-9438-2096 11/08/1950
Victor Vaughan 5394-0493-5334-2306 11/01/1922
Wallace Walding 4179-9794-8333-9893 03/20/1983
Yang Young 6011-8811-4384-2737 03/21/1931
Harrison Dunton 4334-7270-2523-2734 06/11/1998
Lester Pederzani 3689-365602-0936 08/18/1920
Reynaldo Ake 5275-9204-1066-6347 04/19/1985
Leticia Samyn 4198-4752-8724-0202 06/02/1951
Heidi Depner 3448-919116-86886 05/26/1924
Bradley Otoole 3755-358228-33044 05/06/1949
Teddy Litchard 5242-1645-1908-9206 10/03/1969

Open-New Conclusions *

All Data | Alert ID = 3987 x | Clear

Status: All | Assignee: All | Threat Score | Export List | Advanced

Score	Summary	Entity	First Alert	Last Alert	Status
80	Malware W32/ObfusInjectBot.a of Type TRO... #291, 12 alerts, a month old	192.168.2.101	Jun 19 06:52	Jun 19 06:52	New

Conclusions: 1 to 1 of 1 « ‹ Prev 1 Next › » 100 per page

Conclusion #291 Details [New]

Open | Mute | Close | Endpoint Tasks | Label | Comment | Purge

Malware W32/ObfusInjectBot.a of Type TROJAN Detected from 141.251.2.27 to 192.168.2.101 80

ENTITY 192.168.2.101
FIRST ALERT TIME 2019-06-19 06:52:35
LAST ALERT TIME 2019-06-19 06:52:45

WITH MALWARE YES
ENDPOINT ACTIVITY Not Applicable
LABELS [None]

Alerts 12 | Workflow 0 | Asset Details

JUN 19

Showing 4 of 12 alerts. Show all alerts

6:52 Malware W32/ObfusInjectBot.a of Type TROJAN Detected from 141.251.2.27 to 192.168.2.101

Server: 141.251.2.27: 80 | Protocol: HTTP | Client: 192.168.2.101: 55098

Endpoint Activity: Not Applicable
Sandbox Report: Received
Behavior:
MD5: 29ad18b86f1620890b37ff4fd537edae

File Name: FSS_Object-0
File Size 735 KB
Filetype: exe

6:52 Malware Exploit-PDF.b of Type TROJAN Detected from 192.168.2.101 to 217.20.42.224

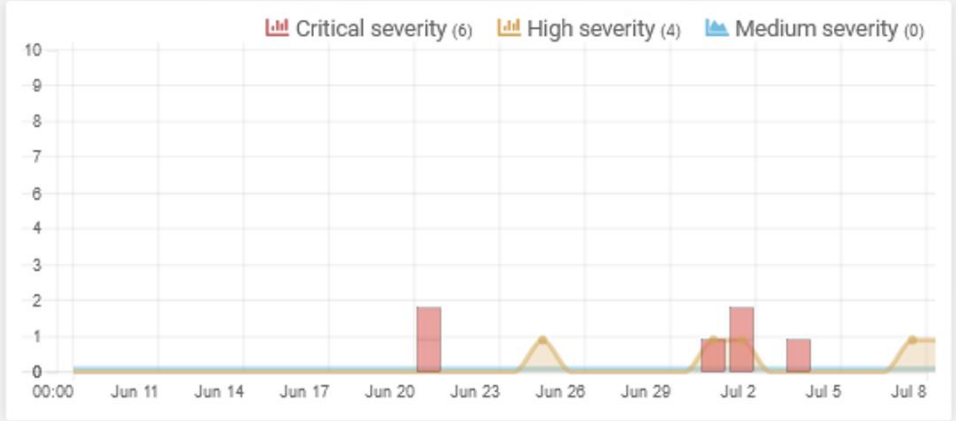
Client: 192.168.2.101: 5123 | Protocol: F.UnknownProtocol* | Server: 217.20.42.224: 34537

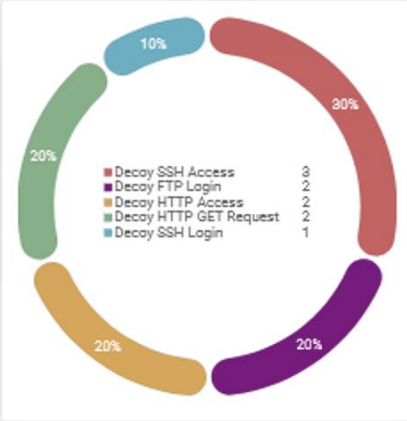
Endpoint Activity: Not Applicable
Sandbox Report: Not Submitted
Behavior:
MD5: c61c231d93d3bd690dd04b6de7350abb

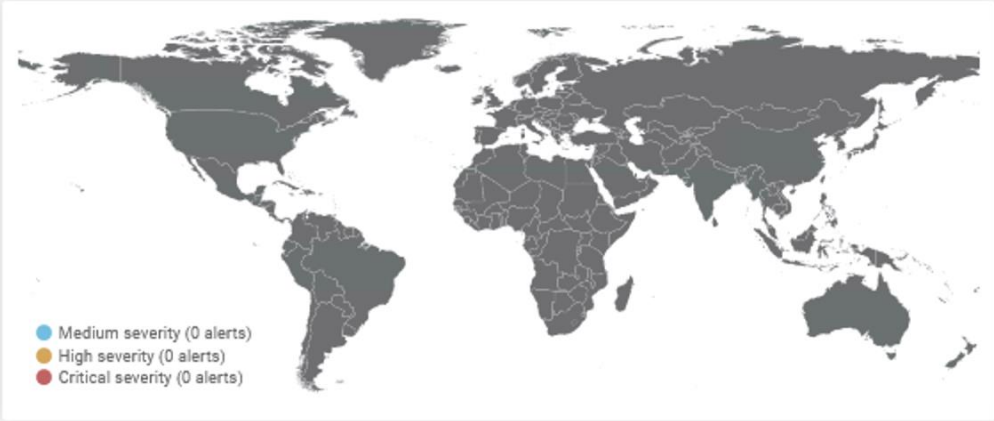
File Name: [Empty]
File Size 128 KB
Filetype: binary

Delete decoy

Decoy - 192.168.200.51 MULTIPLESERVMBP







Edit

Decoy IP: 192.168.200.51
Netbios name: MULTIPLESERVMBP
Comment:
MAC Address: 00:16:41:34:1e:70
Group: PODOLI
Subnet: 192.168.200.0/24

Component: Deception
NIC: eth1
VLAN: 0
Netmask: 255.255.255.0
Gateway: 192.168.200.2

Type: Custom content
Role: Multiple Services
OS: Ubuntu 16.04 (Linux 3.x)
File system: Default

Conclusions & Alerts 6 : 4 : 0 | Deceptive paths | Services 10 | Breadcrumbs 1 | Shared Folders

Add service

Service	Ports	SSL Ports	Login attempts	Successful login	
SSH server		22	9 (3 successful)	Jul 4 2019, 09:50	3 weeks ago
FTP Server	21		1 (1 successful)	Jul 2 2019, 13:10	3 weeks ago
UDP	10		None		
TCP Accept	2049, 512		None		
SMTP server	25	465	None		
Shared Folder	445		None		
Oracle	1521		None		
MySql Server	3306		None		
Web Server	8080	8443	None		
DNS service	53		None		

Define decoy | Save to file | Add multiple decoys

Tags | Filters

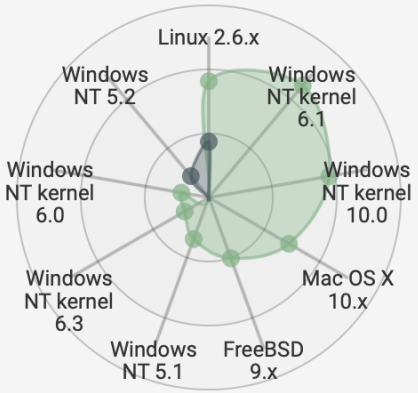
Define Decoys for subnets

Tag decoys | Delete decoys | Filter selected

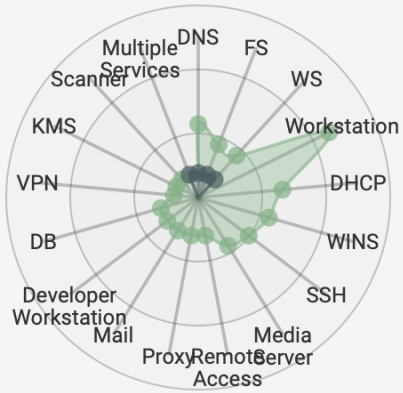
Decoy	Subnet	OS / Vendor	Role	Created on
192.168.13.90 WORKGROUP/hq-it-file090	192.168.13.0/24	Linux 2.6.x CentOs 6.5	Multiple Services 10 services	Jul 8, 17:33 2 weeks ago
192.168.13.163 WORKGROUP/ROUTJQT	192.168.13.0/24	D-Link	Router 4 services	Jul 18, 18:13 Last week
192.168.12.80 WORKGROUP/hq-it-web080	192.168.12.0/24	Windows NT 5.2 Windows 2003	Web Server 6 services	Jul 18, 21:43 Last week
192.168.14.120 WORKGROUP/hq-it-file120	192.168.14.0/24	Linux 2.6.x CentOs 7.2	File Server 3 services	Jul 8, 17:34 2 weeks ago
192.168.13.80 WORKGROUP/DNSIGY	192.168.13.0/24	Linux 2.6.x CentOs 6.5	Domain Name Server 2 services	Jul 10, 09:43 2 weeks ago
192.168.13.29 HQ/ROUTRAE	192.168.13.0/24	D-Link	Router 4 services	Jul 18, 18:13 Last week

Environment | Deception

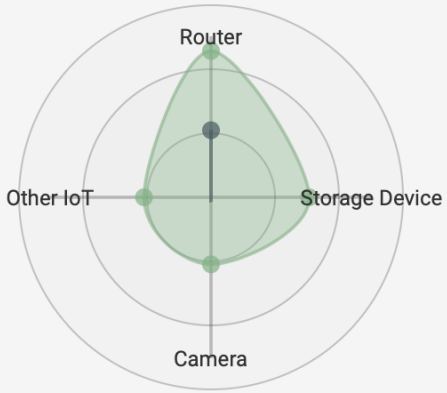
By Operating Systems

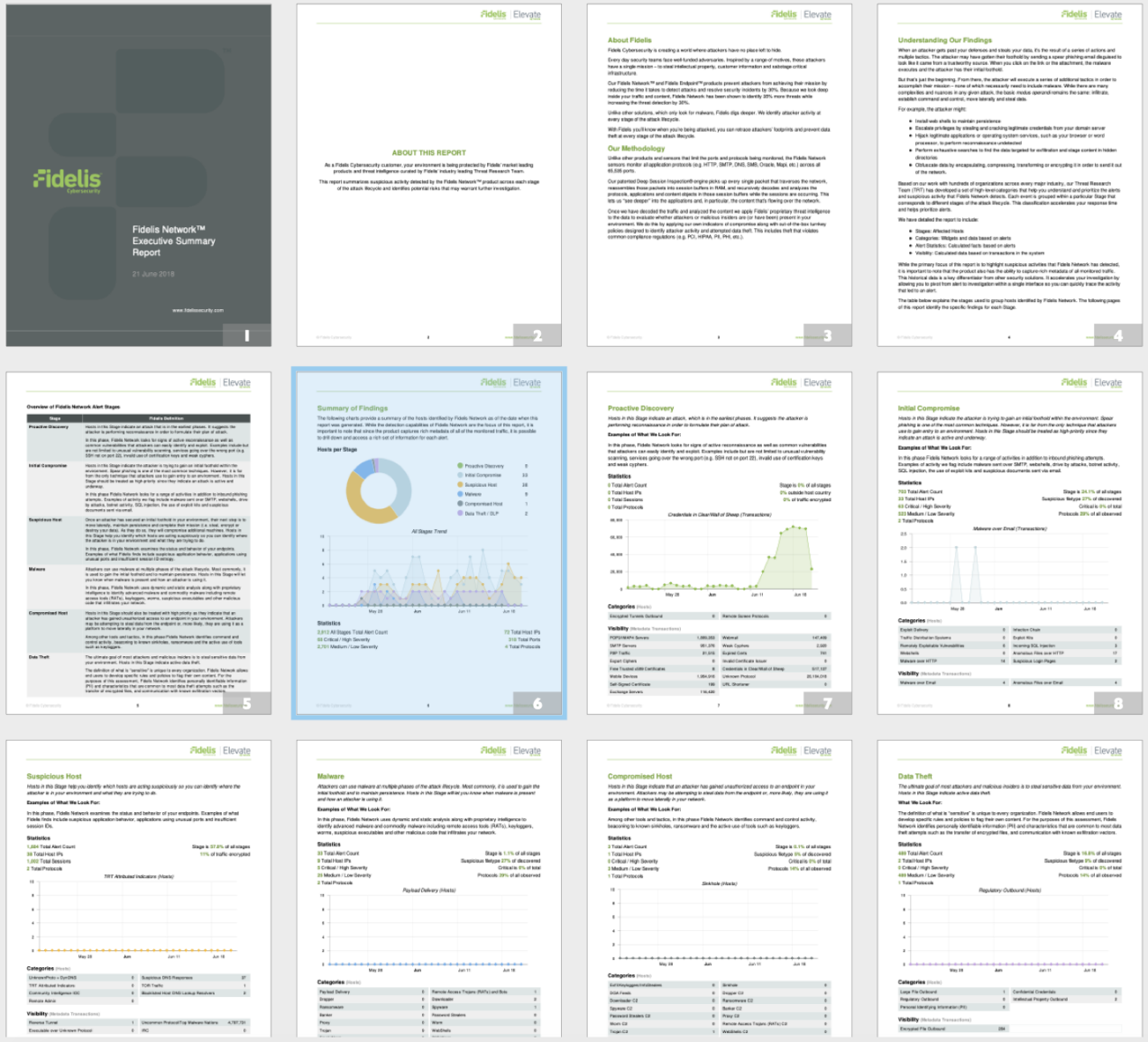


By Computer roles



By IOT devices

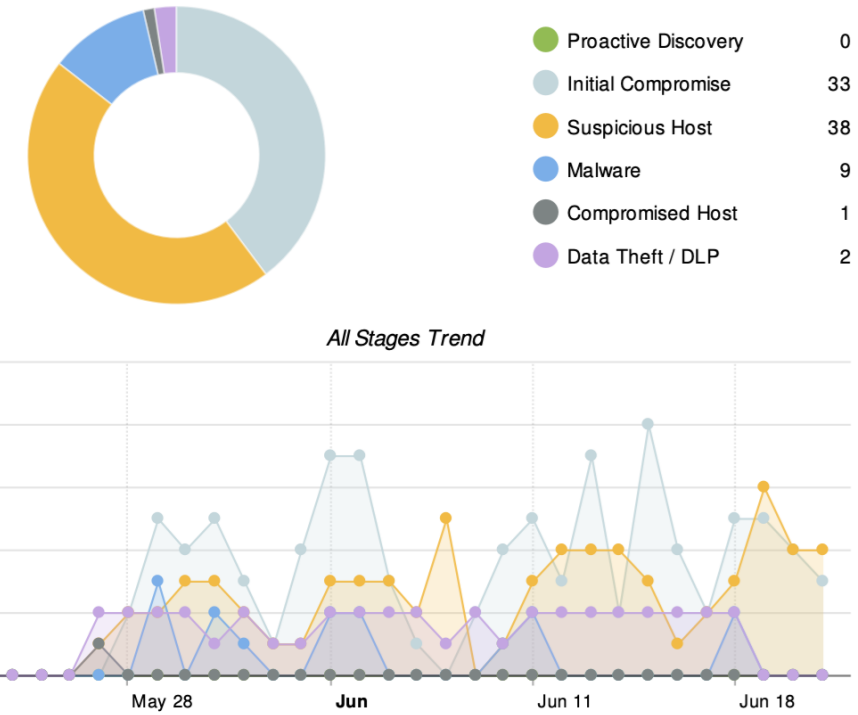




Summary of Findings

The following charts provide a summary of the hosts identified by Fidelis Network as of the date when this report was generated. While the detection capabilities of Fidelis Network are the focus of this report, it is important to note that since the product captures rich metadata of all of the monitored traffic, it is possible to drill down and access a rich set of information for each alert.

Hosts per Stage



Statistics

2,912 All Stages Total Alert Count
68 Critical / High Severity
2,701 Medium / Low Severity
72 Total Host IPs
318 Total Ports
4 Total Protocols

REPORTS
Reports Management
Executive Reports
Network Stats

ADMINISTRATIVE
User Management
System Events
Audit
PCAP Management

DATA SOURCES
Integration Data Links
Asset Information

DETECTION & ANALYTICS
Profiling Networks
Malware Detection
Export

SYSTEM
Components
Deception Components
Version Control

Configuration Wizard

Audit Log

1 - 10 of 12883 « ‹ 1 | 2 | 3 | 4 | 5 › » ⌄

Find: In: Category During Last: All days Search expand all collapse all

ID	Timestamp	User	Category	Action
12883	2019-07-20 12:10:28	admin	audit	Audits

Effect
Page Access
Description
admin accessed audit logs

12882	2019-07-20 12:07:04	admin	report	Reports

Effect
Access Events
Description
admin accessed the report with name: Demo Alerts

12881	2019-07-20 12:06:12	admin	metadata	Meta Search

Effect
Page Access
Description
Metadata Session (detail) page - RelSessionId: 6666397808009867027, Sensor: Direct, Sensor type: IPTRAP, Transaction: 1644543

12880	2019-07-20 12:06:08	admin	metadata	Meta Search

Effect
Page Access
Description
admin accessed Metadata page of collector - Collector, page: metadata list - find metadata

12879	2019-07-20 12:04:19	admin	endpoint	Endpoint Token

Search

Name	Publisher	Version	Highest CVE Score
gettext		0.19.8.1-6ubuntu0.3	7.5 - High
bzip2		1.0.6-8.1	5.1 - Medium
bash		4.4.18-2ubuntu1	4.6 - Medium
accountsservice		0.6.45-1ubuntu1	1.9 - Low
busybox-static		1:1.27.2-2ubuntu3.2	
busybox-initramfs		1:1.27.2-2ubuntu3.2	
bubblewrap		0.2.1-1ubuntu0.1	
bsdutils		1:2.31.1-0.4ubuntu3.3	
bsdmainutils		11.1.2ubuntu1	
brltty		5.5-4ubuntu2.0.1	
branding-ubuntu		0.10	
bolt		0.5-0ubuntu0.18.04.1	
bluez-obexd		5.48-0ubuntu3.1	
bluez-cups		5.48-0ubuntu3.1	
bluez		5.48-0ubuntu3.1	
binutils-x86-64-linux-gnu		2.30-21ubuntu1~18.04	
binutils-common		2.30-21ubuntu1~18.04	

Showing 1 to 100 of 1620 items

‹ 1 2 3 4 ... 17 ›

Endpoints | CVE

CVE	KB	▼Score	Vector	Complexity	Severity	Summary
CVE-2010-0405		5.1	Network	High	Medium	Integer overflow in the BZ2_decompress function in decompress.c in bzip2 and libbzip2 before 1.0.6 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted compressed file.
CVE-2002-0759		5	Network	Low	Medium	bzip2 before 1.0.2 in FreeBSD 4.5 and earlier, OpenLinux 3.1 and 3.1.1, and possibly other operating systems, does not use the O_EXCL flag to create files during decompression and does not warn the

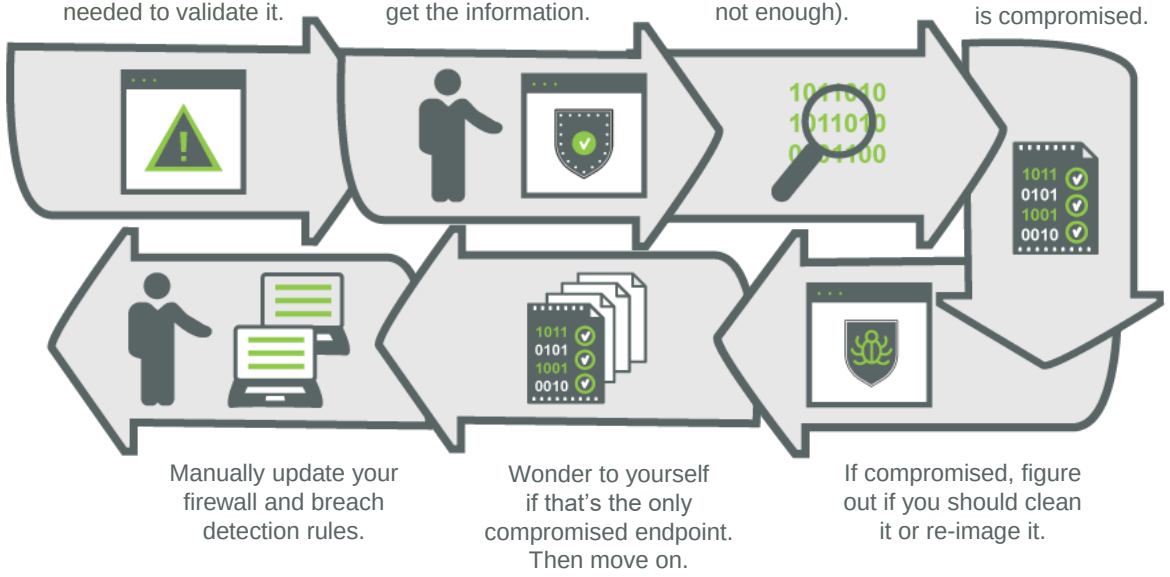
Showing 7 items

Přesnost a rychlost hrají zásadní roli při stanovení priorit, vyšetřování a reakci na incident

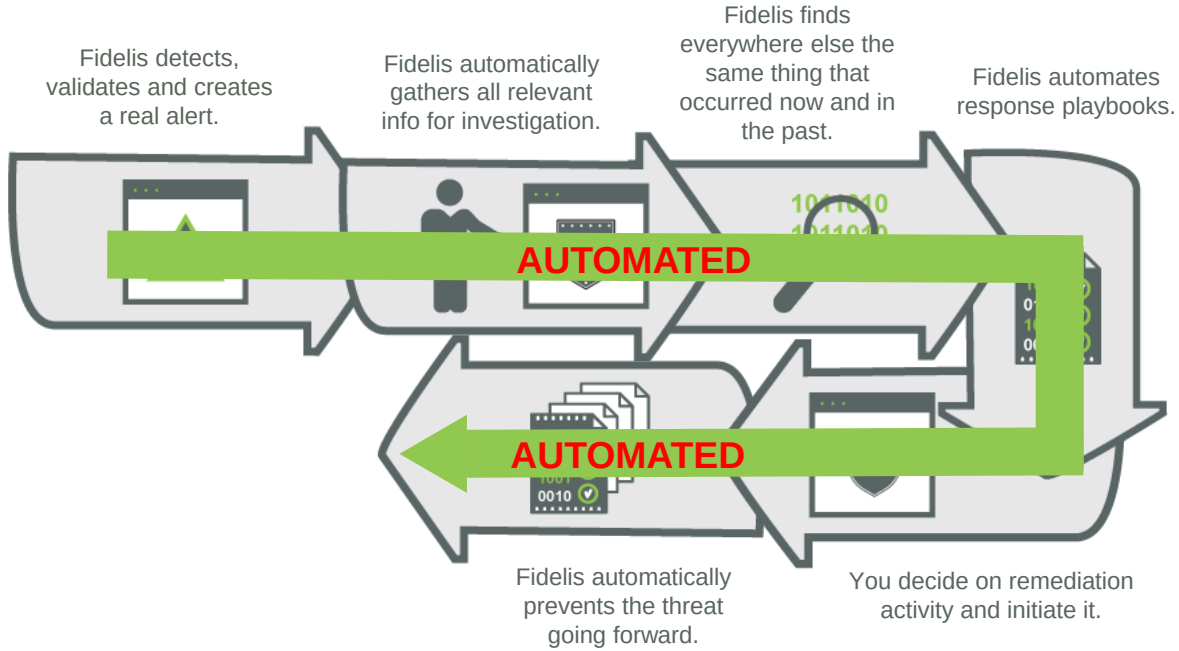
Přesná
Detekce
Analýza

Rychlá
Reakce

BEST CASE
Hodiny - Dny



TYPICKÝ PŘÍPAD
MINUTY
(vs. hodiny - dny)



BEZ FIDELISU

S FIDELISEM

Automated Detection and Response

<table>
<tr><td colspan="11">Fidelis ADR architektura.
Kompletní - Integrovaná - Automatizovaná.</td></tr>
<tr><td rowspan="2">Reakce</td><td colspan="10">Zvýšení efektivity bezpečnostních specialistů pomocí urychlení reakce</td></tr>
<tr><td colspan="3">Jednotné uživatelské rozhraní</td><td colspan="3">Automatizovaná validace alertů</td><td colspan="2">Asistovaná investigace</td><td colspan="2">Asistovaná náprava</td></tr>
<tr><td rowspan="4">Detekce & Prevence</td><td colspan="10">Detekce a prevence během všech fází životního cyklu útoku</td></tr>
<tr><td colspan="4">Statická</td><td colspan="3">Dynamická</td><td colspan="2">Retrospektivní</td><td>Aktivní</td></tr>
<tr><td>Signaturami (Atomická)</td><td>Pravidly (Multidimenzionální)</td><td>Emulací & Heuristicky</td><td>Sandbox</td><td>Endpoint</td><td>Network</td><td>Signatury & Indikátory</td><td>Machine Learning & AI</td><td>Pastičky a návnady</td></tr>
<tr><td colspan="3">Detekce a Prevence v reálném čase</td><td colspan="4">Detekce v reálném čase</td><td colspan="2">Detekce v historii</td><td>Detekce po průniku</td></tr>
<tr><td rowspan="2">Vizibilita</td><td colspan="10">Velmi hluboká vizibilita sítě i koncových bodů (v reálném čase i do historie)</td></tr>
<tr><td colspan="5">Na síti: pakety, celá spojení, obsah a souvislosti, přes všechny porty a protokoly</td><td colspan="5">Na koncovém bodě: procesy, soubory, USB, zranitelnosti, síťová spojení, paměť, registry, pro různé OS</td></tr>
</table>

Další navrhovaný krok: Proof of Concept

Zmapování terénu a nalezení kritických míst a slepých zón ve vaší bezpečnosti

- Vysoce doporučujeme vytvořit si vlastní zkušenost a objevit možnosti řešení
- Kompletní platforma nebo jednotlivé produkty
- Jednoduše a rychle nasaditelné, flexibilně ve VMware nebo jako appliance
- Společně nadefinujeme „kritéria úspěšnosti“ a časový plán

Děkujeme za Vaši laskavou pozornost !

Fidelis™ Cybersecurity