NIC Cloud Connect

Oslo Spektrum
November 7 - 9

NIC Cloud Connect

Tales from Incident Response

- Mikael Nystrom - Truesec
- Microsoft MVP
- Cyber Security Incident Responder

- Viktor Hedberg – Truesec
- Microsoft MVP
- Cyber Security Incident Responder

Fun fact

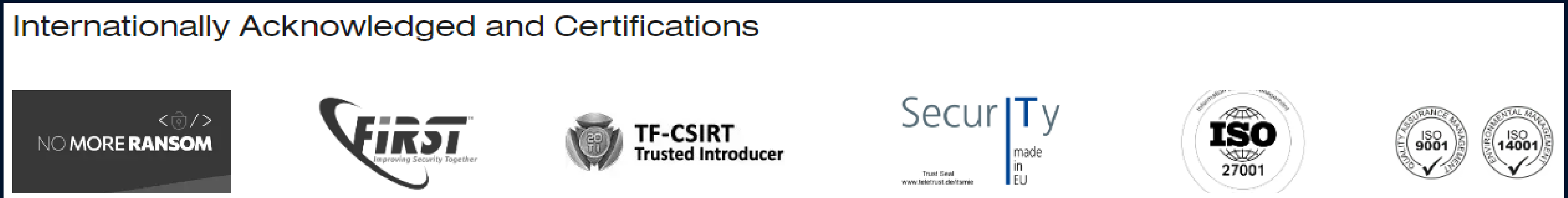
- Lowest Identity Security Score:1.57%
- Highest uptime:834 days
- Longest time to patch: 3 days
- Most time consuming OSD: 2 days
- Oldest Server hardware:
  HP Dl380 G3 with unpatched ILO2
- Oldest F-Secure:915 days

CSIRT

- Statistics:

- Number of incidents yearly 170-200
- Concurrent incidents 10-15
- Hours spent 2023: 35.000hrs and counting

- That gives us “some” insights



Internationally Acknowledged and Certifications

The administrator that really needed to patch...

Story

- “Forced” to run Windows Update
- Used Remote Desktop sessions
- Interactively logging to systems using high value credentials

Outcome

- Fully patched
- Fully ransomware with in 4 hours

Progress

- Primary systems was up within 2 weeks
- Some system was up after 6 months
- Data was lost

Why and what

- RDP is ok, if, used correctly
- Systems should be monitored.
- Patching should be automated
- Pass the hash, Pass the Ticket
- Tiering, Silos, GPOs

Of course we have logging enabled...

Story

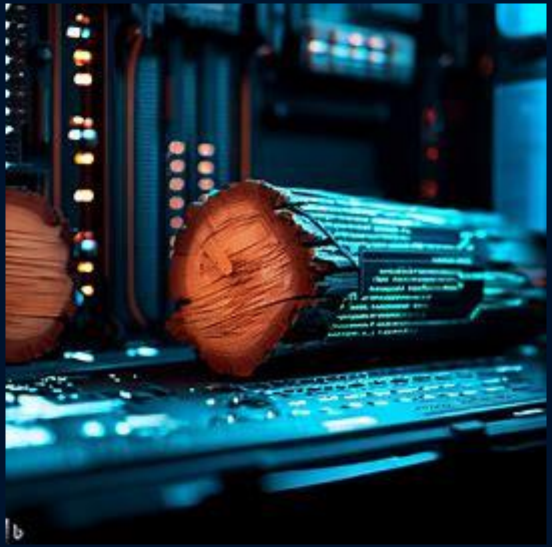
- Standard environment
- Firewall, VPN, Windows, Azure, etc, etc
- Logs stored locally in each system

Outcome

- Customer hacked
- Forensic investigation was not possible

Progress

- No patient Zero
- No entry point



Why and what

- Logs should be enabled
- Logs should be retained for at least 90 -180 days
- Logs should be stored outside and preferable immutable
- Make sure the time is correct
- Make sure all systems are storing logs

Yes, we manage our accounts

Story

- Service accounts with high privs.
- Active Directory is full of old references to admin accounts, servers.
- Bad control and lifecycle management of AD objects

Outcome

- Every service “works”.
- Exposure of Domain Admin on all servers
- The attacker needs to compromise one (1) server

Progress

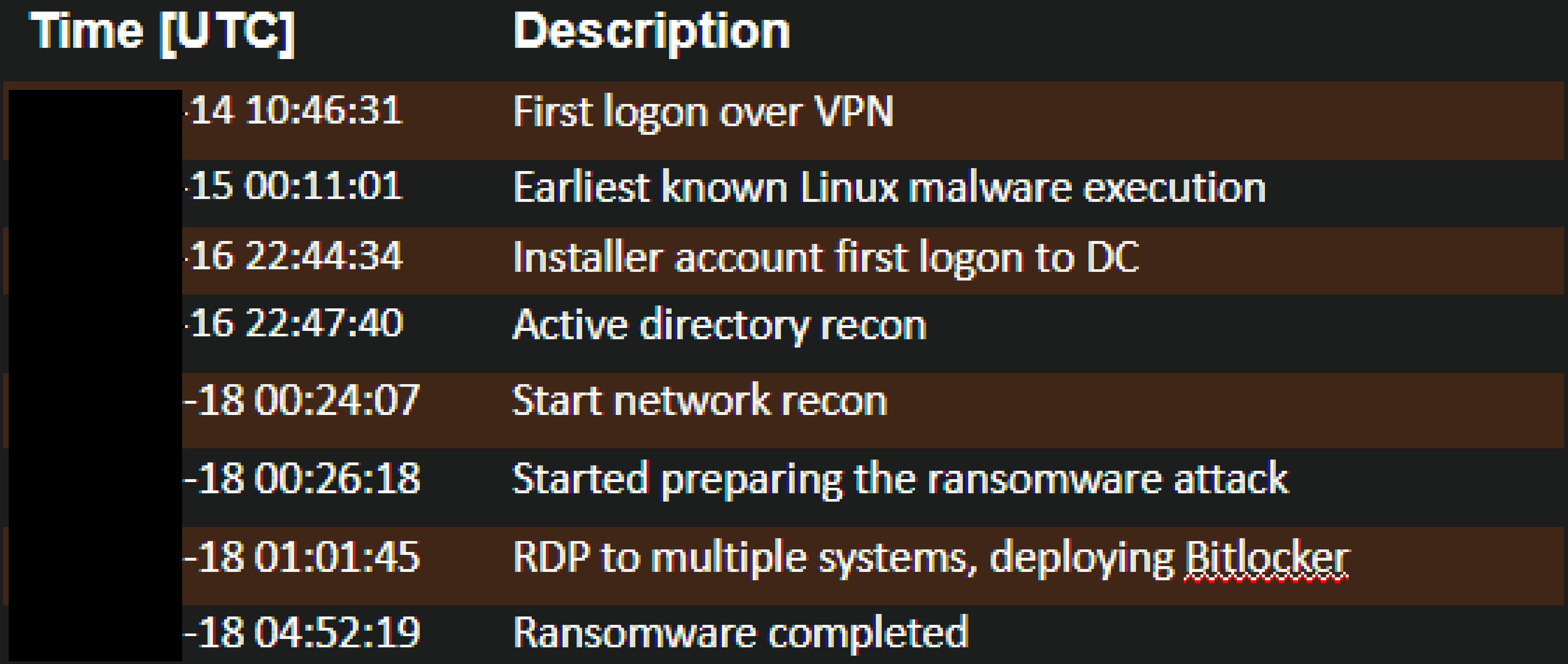
- Restore from backup (not all systems)
- Recover from datamining (some systems)
- Primary functions was up after 2 weeks
- Data was lost

Why and what

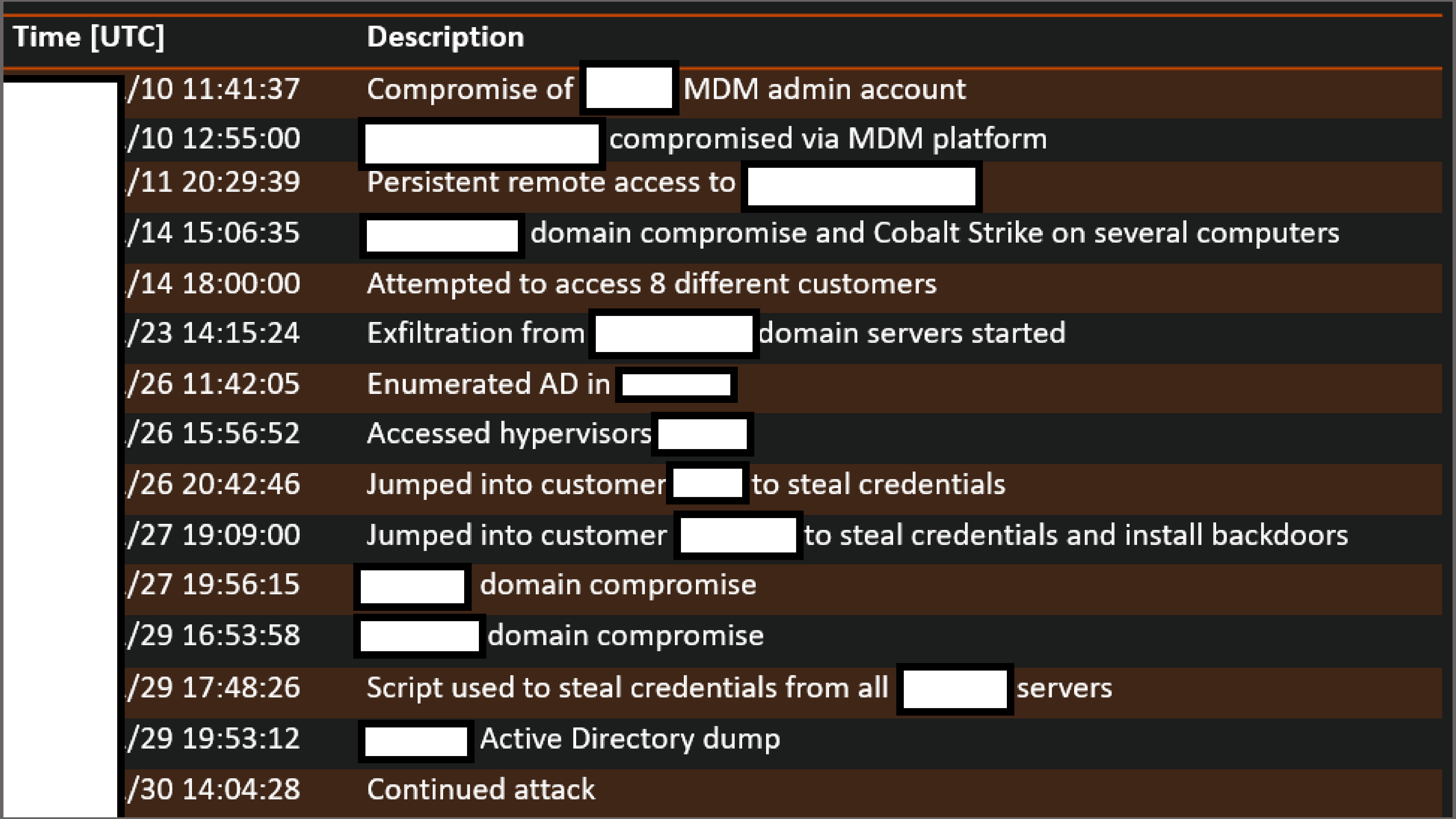
- Admin accounts should not be deleted
- Service accounts should not be domain admins
- Service accounts should not be local admins everywhere
- Former admin accounts should be disabled, parked, stripped, renamed and never used again, but kept forever
- Use gMSA accounts, Local System, Local Service, Network Service, Domain User
- Each services should have its own account
- Service Accounts does not need to logon interactively
- User accounts does not need to logon as a Service

nic Cloud Connect

Samples



Time [UTC]	Description
[redacted]-14 10:46:31	First logon over VPN
[redacted]-15 00:11:01	Earliest known Linux malware execution
[redacted]-16 22:44:34	Installer account first logon to DC
[redacted]-16 22:47:40	Active directory recon
[redacted]-18 00:24:07	Start network recon
[redacted]-18 00:26:18	Started preparing the ransomware attack
[redacted]-18 01:01:45	RDP to multiple systems, deploying Bitlocker
[redacted]-18 04:52:19	Ransomware completed



Time [UTC]	Description
[redacted]/10 11:41:37	Compromise of [redacted] MDM admin account
[redacted]/10 12:55:00	[redacted] compromised via MDM platform
[redacted]/11 20:29:39	Persistent remote access to [redacted]
[redacted]/14 15:06:35	[redacted] domain compromise and Cobalt Strike on several computers
[redacted]/14 18:00:00	Attempted to access 8 different customers
[redacted]/23 14:15:24	Exfiltration from [redacted] domain servers started
[redacted]/26 11:42:05	Enumerated AD in [redacted]
[redacted]/26 15:56:52	Accessed hypervisors [redacted]
[redacted]/26 20:42:46	Jumped into customer [redacted] to steal credentials
[redacted]/27 19:09:00	Jumped into customer [redacted] to steal credentials and install backdoors
[redacted]/27 19:56:15	[redacted] domain compromise
[redacted]/29 16:53:58	[redacted] domain compromise
[redacted]/29 17:48:26	Script used to steal credentials from all [redacted] servers
[redacted]/29 19:53:12	[redacted] Active Directory dump
[redacted]/30 14:04:28	Continued attack

Single Sign is awesome, but not for everyone

Story

- All systems are well connected.
- Administrators have a single admin account
- The admin account(s) was Domain Admin, Global Admin, and vSphere admin

Outcome

- The administrators have a very easy way to work on daily basis.
- The attacker gained access from a password spray and became the “almighty” easy.
- The attacker encrypted the VMs using a GPO as well as the storage in VMware

Progress

- Restore from backup (not all systems)
- Recover from datamining (some systems)
- Primary functions was up after 2 weeks
- Data was lost

Why and what

- Administrative logons should be isolated.
- The network should be segmented
- Trusts, PAWs, Silos, Tiering, MFA

Isolation is lonely

Story

- All systems are well connected.
- The administrator might use different admin accounts.
- From one single device it is possible to “ping” everything

Outcome

- The attacker got in a laptop, scanned the network
- Found VMware, Hyper-V, ILO/Idrac
- Eventually managed to get in to Vmware
- Launch the ransomware attack.

Progress

- Restore from backup (a few systems)
- Recover from external consultans (randomly stored data on usb devices)
- Primary functions was up after 2 weeks
- Data was lost

Why and what

- Isolation should be in place for Hypervisors, Backup, Monitoring
- Applies to both network and authentication
- Multiple PAWs, (one for each env)

The backup solution with no capability to restore the data

Story

- Backup solution was running in WORKGROUP
- Data was stored on NAS devices
- NAS Device password was used in other locations

Outcome

- Backup was working as expected
- The attacker scanned the network and found the NAS devices, erased them, installed backdoors..

Progress

- The attacker was “unlucky”, they destroyed the server that was used in the attack, so many VMs was unaffected.
- Rebuild many functions

Why and what

- Backup and restore is the last line of defense!
- It is not a DR solution!
- It should be a hole in the wall sometimes referred as a diode-based solution

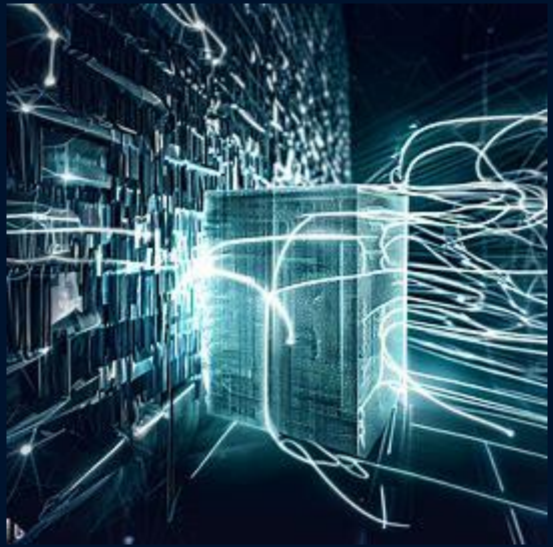
Next Generation Firewall's are awesome, but...

Story :

- Advanced firewalls was installed, Windows firewall was disabled
- No need of EDR or AV, since the advanced firewalls should detect anything

Outcome :

- The attacker gained access to the network using a test account in the VPN solution
- The attacker scanned the network and found the NAS devices
- The attacker exported the data on the dark web, formatted the data disks and installed backdoors and executed the ransomware attack.



Why and what

- The network detection happens after the systems are attacked
- The “only” network traffic that is fairly easy to detect is C2 communication
- It makes it harder to work for the administrators.
- When the advanced firewall detects traffic, the attack has already begun

The VPN solution that gave us everything

- The VPN solution that gave us more then we could possibly imagine..

VPN solutions...

- The attacker “bought” a credential online and logged in, full network access to everything.
- The attacker used a vulnerability in the VPN solution, full network access to everything
- The attacker tried with the default credentials in VPN solution, full network access to everything
- The attacker “asked” a user for the VPN credentials, full network access to everything
- The account VPNTest has the password of VPNTest, and no MFA , full network access to everything

Solution

- VPN should only be used if the devices is managed.
  - Controlled by EDR, MDM, etc
  - Joined to the Domain
- VPN should only allow needed communication, very few users needs to logon to the ESXi hosts
- VPN should be something like AOVPN, certificate based, machine based.

Note: Once the attacker is in, they invest in scanning to find out what you have... #lifeisunfair

The solution that is not used, except by the threat actors...

- Exposed Exchange for collaboration, should have been decommission a few years ago
- Exchange hybrid, 3 more mailboxes to move, but
- The LDAP port is published on the Internet, something was using it...

Solution is not used anymore

- The solution was running, fully connected
- The attacker used a Web Shell on the Exchange Server
- The SharePoint services account was Domain Admin
- The system was terminated on paper 5 years ago...
- The attacker could continue to other systems, since there was full trusts to several other domains

Solution

- You need to maintain systems until they day they are turned off

Note: Attackers don't care what system they can use to get access... #lifeisunfair

We patch everything,

except, that server, that VPN, that firewall, that ILO, that switch, that Idrac, and that client...

- Patch solution was in place for Windows Clients and for most servers
- Solution was automated with exceptions

Patching is not always easy...

- Hardware was in general never patched since first power on (15-20 years)
- VPN was not patched for more then 5 years
- The attacker used a nice feature named “Create VPN account without being logged on”
- Connected to the VPN solution for almost 3 months, the attacker could get access to Active Directly and launch the attack

- Primary functions was up after 2 weeks
- Restore using the “I think I have a copy of that” as well as regular backup (external)
- Rebuild many functions
- Data was lost

Solution

- Minimize everything, Make life easier
- If the network adapter is connected
    - it can be hacked
    - it will contain security issues
- You need to maintain it until it is turned off

Ten immutable laws of cyber security

#1 Nobody believes anything bad can happen to them, until it does.

#2 Security only works if the secure way also happens to be the easy way.

#3 If you don't keep up with security fixes, your network won't be yours for long.

#4 It doesn't do much good to install security fixes on a computer that was never secured to begin with.

#5 Eternal vigilance is the price of security.

Ten immutable laws of cyber security

#6 There really is someone out there trying to guess your passwords.

#7 The most secure network is a well-administered one.

#8 The difficulty of defending a network is directly proportional to its complexity.

#9 Security isn't about risk avoidance; it's about risk management.

#10 Technology is not a panacea.

Ten immutable laws of cyber security

These laws were written, prior to year 2000

And we are still struggling with these fundamentals...

“The threat actor does not care about your security, they care about your weakness, and they only need to find one, tiny hole, one time”

Thank you!