Attacking Prey on Uncertainty: How to Fail at Threat Detection

February 7th, 2020
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

1001 DAYS IN THE LIFE OF A THANKSGIVING TURKEY

SOURCE: Nassim Taleb, "The Black Swan"
Are You the Farmer or the Turkey?

BELIEVES
COMPROMISE IS INEVITABLE

HAS 100K SENSITIVE
FILES OPEN TO EVERYONE
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?
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
Step 1: Find accounts with Service Principal Names
Step 2: Get their Kerberos tickets

* 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-D31B6C55EB04/hub-ldu.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 3: Which of these accounts have elevated privileges?
Step 4: Let’s crack one (offline)
Step 5: Let’s use our new account to find some files
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
Especially when your security vendors do it, too!

Domain: 3.1o19sr00n68...67226sorn3.p29p3...506rp979s.***581p.i.00.s.****hosxl.net
Record type: TXT
How quickly & accurately can you answer the most important question:

“Is our data safe?”
The CISO / Board Disconnect

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
- Potential ticket harvesting attack

DATA ACCESS
- Abnormal access to sensitive data by a service account

NETWORK & DNS
- First time access to the internet by a service account
- Data exfiltration attempt via DNS tunneling

BackupService logs into Jim-PC for the first time
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**
- Phishing emails w/ attachments
- Dropped malicious VBS file
- Loads payload with BITSAdmin

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

**PERSISTENCE**
- 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

Qbot malware resurfaces in new attack against businesses
This new persistent and difficult-to-detect Qbot version is designed to steal financial information.

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 10  

SHARE ▼
How do we succeed as defenders?
We know what attackers want: it's almost always data
What if security started with data?

We’d know where our sensitive data lives
We’d monitor it for abuse
Only the right people would have access
We’d efficiently sustain our secure state
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

DEPLOY
- Deploy Varonis
- Discover privileged accounts
- Classify sensitive data
- Baseline activity
- Prioritize risk

OPERATIONALIZE
- Enable alerts and automate response
- Connect to SIEM
- Create and test incident response plans
- Operationalize reporting
- Apply labels
- Index for compliance

FIX
- Remediate exposed sensitive data
- Eliminate remaining global access groups
- Eliminate AD artifacts
- Quarantine sensitive data
- Archive/delete stale data

TRANSFORM
- Identify and assign data owners
- Simplify permissions structure
- Enable data-driven reporting

AUTOMATE
- Automate authorization workflow via Data Owners
- Automate periodic entitlement reviews
- Automate disposition, quarantining, policy enforcement

IMPROVE
- Regularly review risks, alerts and processes to ensure continuous improvement
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