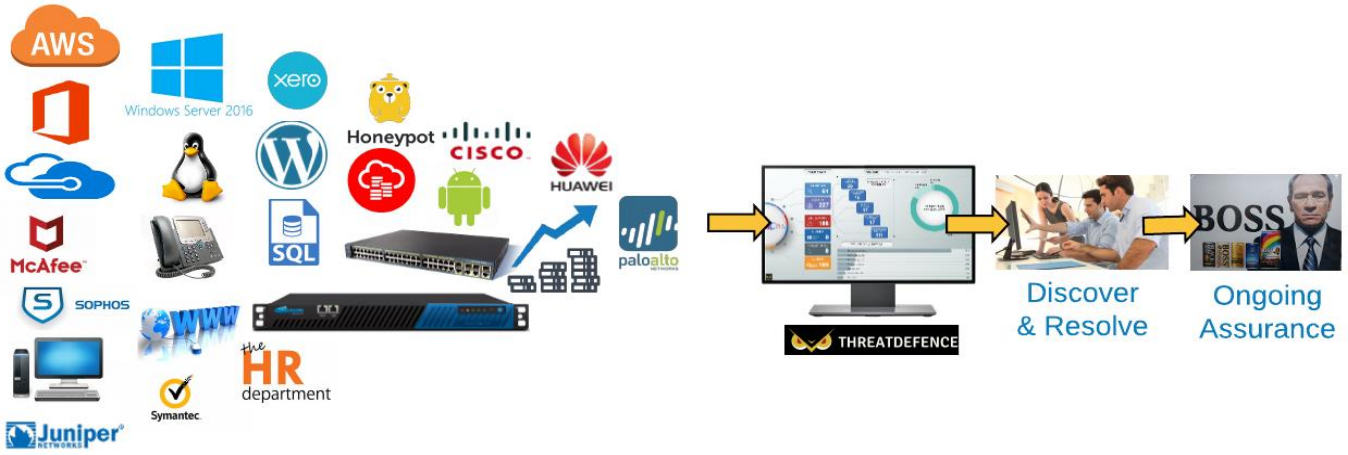
Providing opportunities to prevent breaches.

What if largest global victims had ThreatDefence?



29 November 2018 Commercial in Confidence

Table of Contents

Summary

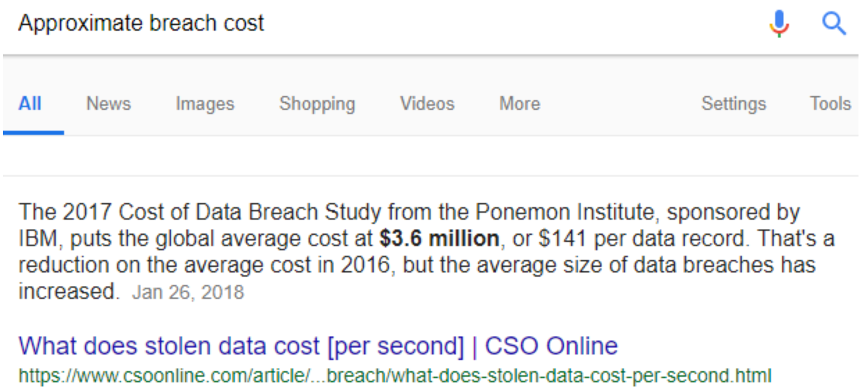
Target, Sony, NASA, Tesla and Uber were investing millions in their cybersecurity products and programs. Their security budgets rivalling the size of a small country's GDP, serviced by the top security providers in the world. It was never about the money. They lacked care and effective visibility.

All these breaches were easily preventable. It was not because hackers are so good, but businesses lack controls and visibility.

ThreatDefence provides an opportunity to prevent breaches. The table below outlines how Threat Defence is expected to perform under breach in your organization:

BREACH STAGE	
BEFORE:	Seconds after powering on, it will start exposing the lack of controls and other risks such as connections to malicious sites.
DURING:	Alerts are generated during exploitation, depending on the attack sophistication and the noise made by the attack.
AFTER:	Categorical records retained. Even if the breach is not detected, it will be recorded, saving thousands in response work.

$3.6ml



Approximate breach cost

The 2017 Cost of Data Breach Study from the Ponemon Institute, sponsored by IBM, puts the global average cost at **$3.6 million**, or $141 per data record. That's a reduction on the average cost in 2016, but the average size of data breaches has increased. Jan 26, 2018

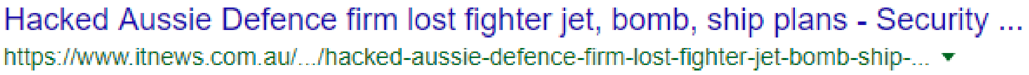
What does stolen data cost [per second] | CSO Online

https://www.csoonline.com/article/...breach/what-does-stolen-data-cost-per-second.html

This documents reviews some of the high-profile breaches and provides an analysis of how the breach could have been detected if the victim organizations were using ThreatDefence.

By utilizing a system like ThreatDefence, organizations have an opportunity to prevent breaches, maintain their brand reputation and save thousands on the response.

1. Attackers infiltrate Australian Defence Contractors



Hacked Aussie Defence firm lost fighter jet, bomb, ship plans - Security ...
https://www.itnews.com.au/.../hacked-aussie-defence-firm-lost-fighter-jet-bomb-ship-...

When:	Oct 2017
Impact:	Lost sensitive documents on Joint Strike fighter and P-8 plane.

1.1 Breach summary

A hacked Australian Defense subcontractor lost 30GB of "commercially sensitive" documents on projects including the Joint Strike Fighter (JSF) program and the P-8 Poseidon “submarine killer” plane, as well as detailed designs of Australian Navy ships.

1.2 Narrative

An internet facing help desk server was running outdated software that contained an “arbitrary file upload vulnerability”, which enabled the attacker to upload a web-based management shell. From there the attacker uploaded several tools to extract cached domain credentials and local Administrator passwords and move laterally throughout almost every Windows server on the network with full privileges.

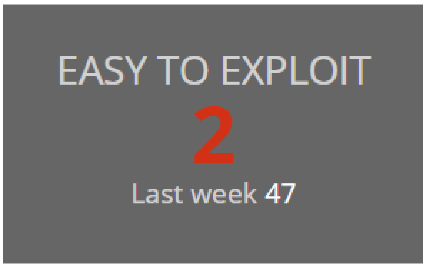
Confidential documents and email archives were compressed into RAR archives copied into a web-accessible directory for download over HTTPS.

1.3 If they had ThreatDefence:

Very early warning, pre-exploitation stage:

- Minutes after deployment the sensors would have detected the lack of a reverse proxy for internet facing applications. Lack of critical control.

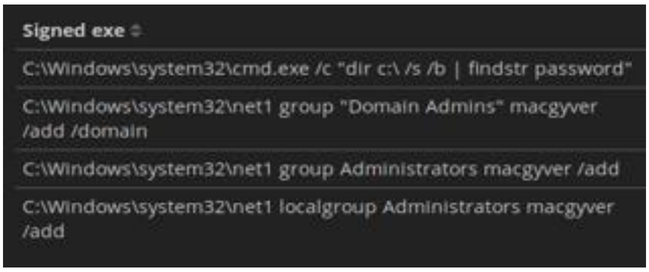
- The built-in vulnerability scanner would have detected the vulnerable help-desk version during the weekly scans. It is a critical vulnerability which would immediately alert in the dashboard and send an email alert.



Post-exploitation stage:

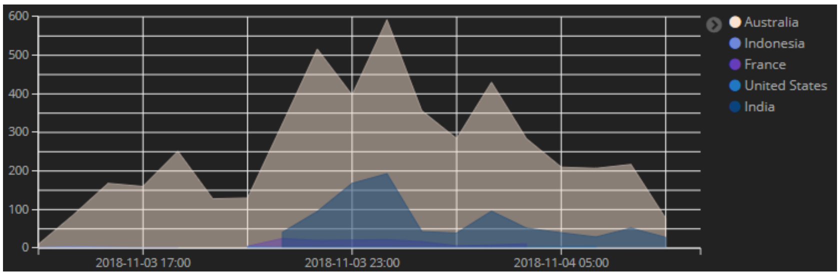
- Tools used to extract and dump cached domain and local administrator credentials (such as Mimikatz) would be recorded and alert on the dashboard.

- Tools used for lateral movement and pivoting to other systems (such as psexec) are recorded and alerted upon via the endpoint agent, even when AV software fails to detect them.

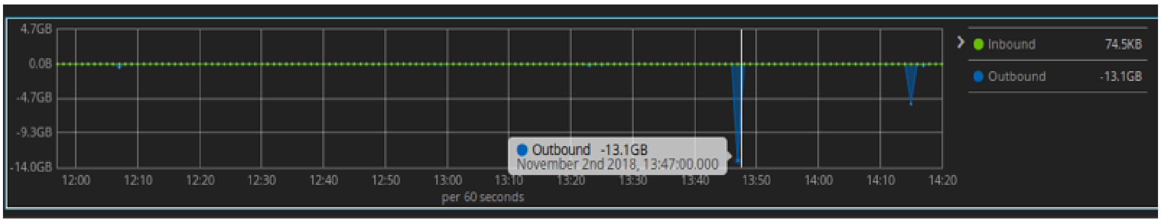


```
Signed exe ⇕
C:\Windows\system32\cmd.exe /c "dir c:\ /s /b | findstr password"
C:\Windows\system32\net1 group "Domain Admins" macgyver
/add /domain
C:\Windows\system32\net1 group Administrators macgyver /add
C:\Windows\system32\net1 localgroup Administrators macgyver
/add
```

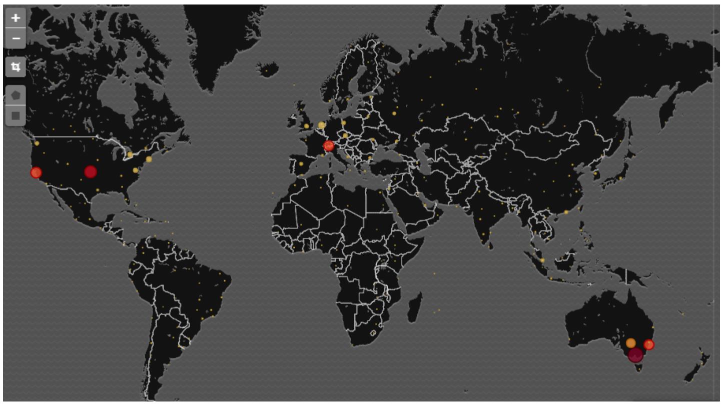
- Login events and new user creations are automatically recorded and alertes on based on severity. This includes geo locations, device UID’s, user agents and other categorical records.

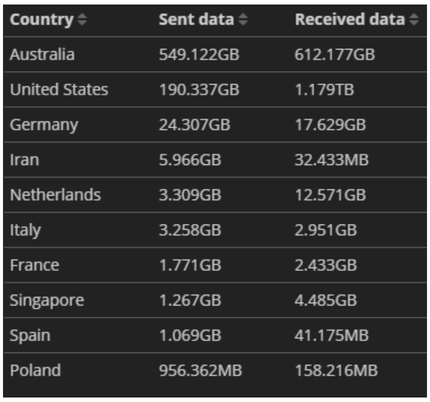


- Sudden spikes in traffic from web servers would be recorded by the NetFlow module and flagged as abnormal especially in the case of exfiltrating large RAR archives:



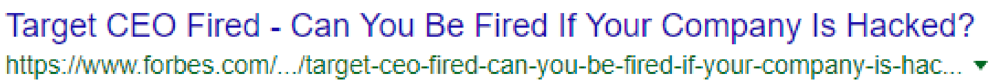
- Web server logs are inspected by TD to detect unexpected files and web directories being accessed, including web shells and archives.





Country	Sent data	Received data
Australia	549.122GB	612.177GB
United States	190.337GB	1.179TB
Germany	24.307GB	17.629GB
Iran	5.966GB	32.433MB
Netherlands	3.309GB	12.571GB
Italy	3.258GB	2.951GB
France	1.771GB	2.433GB
Singapore	1.267GB	4.485GB
Spain	1.069GB	41.175MB
Poland	956.362MB	158.216MB

2. Target credit card breach



Target CEO Fired - Can You Be Fired If Your Company Is Hacked?
https://www.forbes.com/.../target-ceo-fired-can-you-be-fired-if-your-company-is-hac... ▾

When:	Late 2013
Impact:	The breach cost over $300 million, CEO fired.

2.1 Breach summary

Hackers gained access to Target's network by first stealing credentials from a third-party heating and ventilation company, via a spear phishing attack, who had access to Target's network to monitor and maintain their systems.

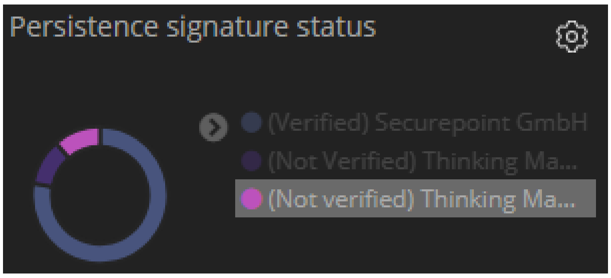
2.2 Narrative

Using the stolen credentials, attackers installed the malware on the point of sale (POS) devices. The malware disguised itself as a legitimate product and copied and sent the stolen credit card data to locally compromised Target servers. It used clever techniques to disguise itself, by sending traffic only during business hours.

Finally, several weeks later, the data started leaving Target's network and was sent to Moscow.

2.3 If they had ThreatDefence

- Endpoint agents would detect malware masquerading as legitimate tools by inspecting false or missing signatures and alerting. Something which AV vendors still can't detect.



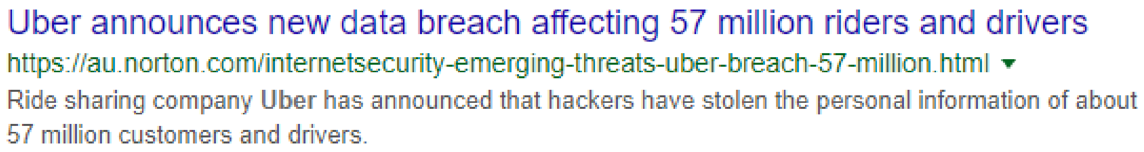
Persistence signature status

● (Verified) Securepoint GmbH
● (Not Verified) Thinking Ma...
● (Not verified) Thinking Ma...

- Windows login analysis would detect user accounts logging into endpoints or servers where they have never logged in before, generating alerts.

- Network flow module would detect abnormal data transfers to Moscow and would generate alerts.

3. Uber tried to cover up the mega breach



Uber announces new data breach affecting 57 million riders and drivers

https://au.norton.com/internetsecurity-emerging-threats-uber-breach-57-million.html ▾

Ride sharing company Uber has announced that hackers have stolen the personal information of about 57 million customers and drivers.

When:	Late 2017
Impact:	Hackers stole 57 million accounts, cost $204 million, CSO Fired

3.1 Breach summary

Hackers were able to access Uber's GitHub account via phished credentials, where they found username and password credentials to Uber's AWS account. Uber tried to cover-up the breach by "bribing" its hackers to delete their data, which resulted in massive regulatory fines.

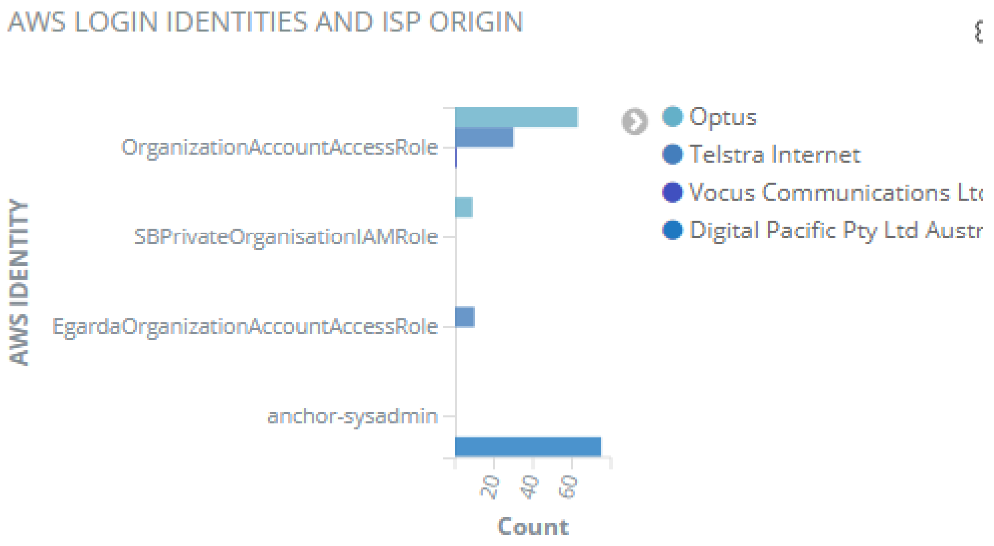
3.2 Narrative

Hackers accessed Uber's GitHub account where they found credentials to Uber's AWS account. Those credentials should never have been on GitHub but attackers were able to use these AWS credentials to download records on 57 million customers and drivers.

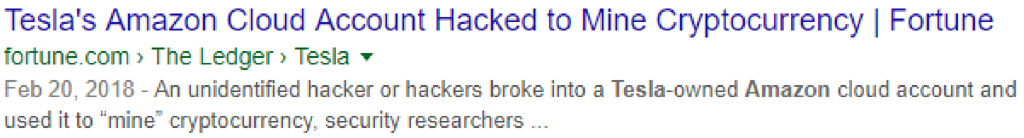
3.3 If they had ThreatDefence

- ThreatDefence has built in top phishing and malware inspection by utilising Google's safe browsing Intel, amongst other intel threat source feeds

- ThreatDefence can record the source location of all logins and API calls to AWS and alert on logins or API activity from an unexpected location:



4. Tesla servers ended up mining cryptocurrency



Tesla's Amazon Cloud Account Hacked to Mine Cryptocurrency | Fortune

fortune.com › The Ledger › Tesla ▾

Feb 20, 2018 - An unidentified hacker or hackers broke into a **Tesla**-owned **Amazon** cloud account and used it to "mine" cryptocurrency, security researchers ...

When:	Feb 2018
Impact:	Hackers deployed crypto mining operations inside Tesla's network

4.1 Breach summary

Hackers "CryptoJacked" Tesla's AWS account and were able to mine virtual currency undetected, entirely at Tesla's expense, also potentially exposing customer information in S3.

4.2 Narrative

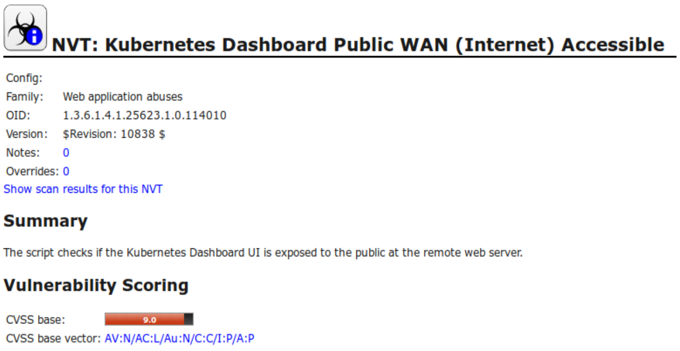
Tesla was breached via a publicly exposed Kubernetes console which lacked login credentials. From here attackers were able to deploy containers with cryptocurrency mining applications in Tesla's AWS account.

The attackers cleverly hid their command and control server IPs behind IP addresses hosted by security firm Cloudflare. They also configured the mining software to use a non-standard port to reach the Internet. This made the illicit mining harder to detect and lower the chances of it being shut down.

4.3 If they had ThreatDefence

Early warning, pre-exploit:

The built-in vulnerability scanner would have detected the publicly exposed K8s console. It is assigned a CVSS of 9/10 a Critical vulnerability which immediately alerts in the dashboard.



NVT: Kubernetes Dashboard Public WAN (Internet) Accessible

Config:	
Family:	Web application abuses
OID:	1.3.6.1.4.1.25623.1.0.114010
Version:	$Revision: 10838 $
Notes:	0
Overrides:	0

Show scan results for this NVT

Summary

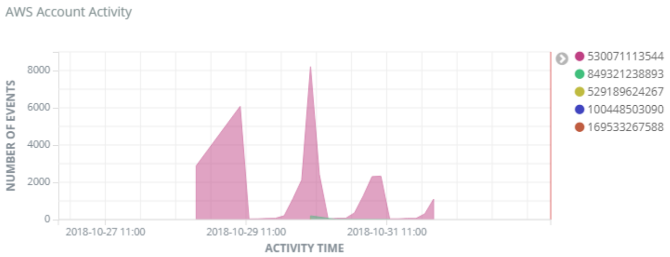
The script checks if the Kubernetes Dashboard UI is exposed to the public at the remote web server.

Vulnerability Scoring

CVSS base:	9.0
CVSS base vector:	AV:N/AC:L/Au:N/C:C/I:P/A:P

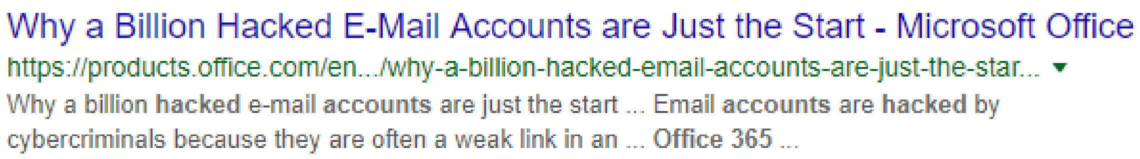
Post-exploit:

The sudden spike in instances created in Amazon would also be recorded by TD (via Cloudtrail) and flagged as an abnormality.



The use of non-standard port to reach the internet suggests Tesla had no outgoing firewall access controls, triggering "Firewall NIST control" alert.

5. 20% Azure Office 365 accounts compromised



Why a Billion Hacked E-Mail Accounts are Just the Start - Microsoft Office
https://products.office.com/en.../why-a-billion-hacked-email-accounts-are-just-the-star... ▾
Why a billion hacked e-mail accounts are just the start ... Email accounts are hacked by cybercriminals because they are often a weak link in an ... Office 365 ...

When:	Aug 2018
Impact:	Successful logins to Office 365 accounts from Nigeria

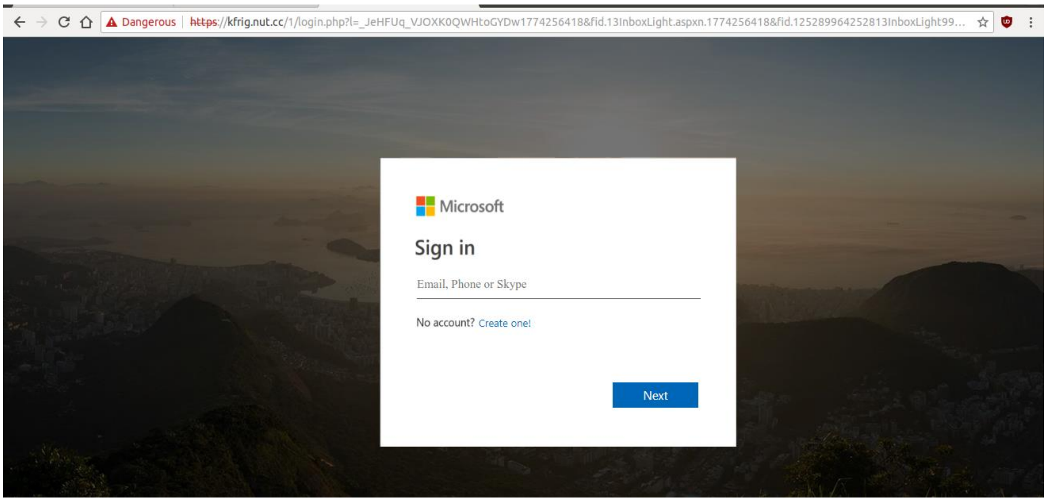
5.1 Breach summary

After enabling the Office 365 module in an iconic Australian public organisation, ThreatDefence began to see corporate accounts being accessed from Nigeria.

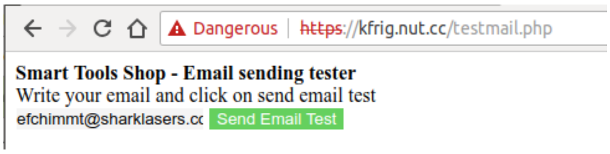
5.2 Narrative

Office 365 accounts were being successfully logged into by Nigerian cybercriminals. The aim is to use corporate accounts as an accessory in cybercrime, such as phishing campaigns. The customer requested a post-breach investigation and our analysts replayed the entire lifecycle of the attack:

An email attachment infected one PC, about 900ms later, 90 more PC's started making a HTTPS connection to a phishing website in India. The phishing website kfrig.nut(dot)cc was designed to harvest credentials from Office 365, this is screenshot obtained during the investigation. The site was a well-designed clone of the Office365 login page and was purposefully failing the first authentication attempt, then redirecting users to office.com to masquerade the fact.


Dangerous | ~~https~~://kfrig.nut.cc/1/login.php?l=_JeHFUq_VJOXK0QWHtoGYDw1774256418&fid.13InboxLight.aspxn.1774256418&fid.125289964252813InboxLight99...
Microsoft
Sign in
Email, Phone or Skype
No account? Create one!
Next

Attackers scripts and tools were identified and analysed to fine-tune defences.



Dangerous | ~~https~~://kfrig.nut.cc/testmail.php

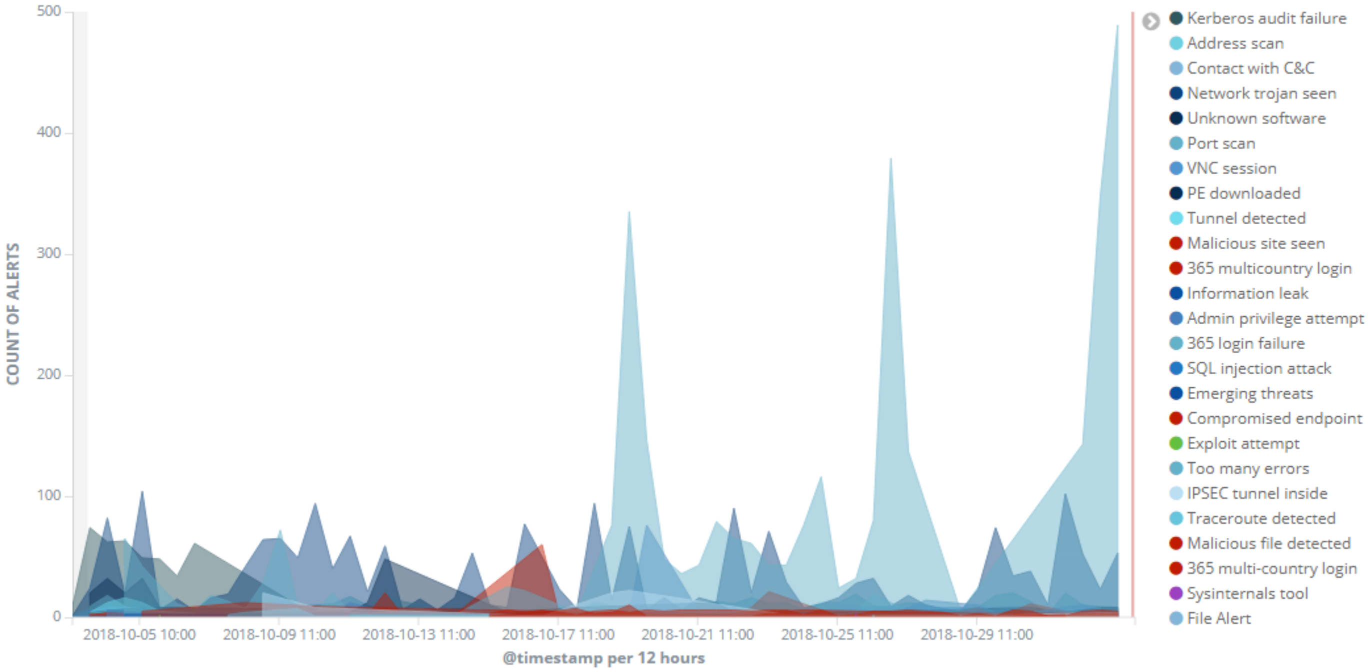
Smart Tools Shop - Email sending tester
Write your email and click on send email test
efchimmt@sharklasers.cc Send Email Test

When ThreatDefence analysts validate incidents, it returns complete forensic information with zero false-positives.

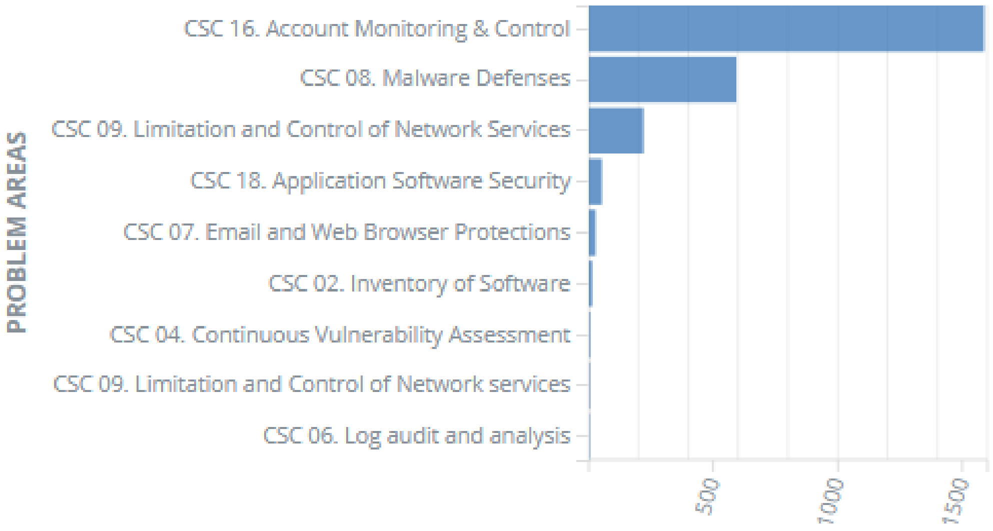
6. About ThreatDefence's use case module

Based on a process that constantly runs in background hunting for threats, what typically takes months for ten full-time auditors merely takes seconds. Typically, it searches over 50 million events and exposes risks to be remediated. New use cases and algorithms are constantly being added.

POTENTIAL RISKS DETECTED AT THESE TIMES:



The discovered threats are categorised according to SANS's critical 20 controls, derived from CIS (Centre for Internet Security). The categories provide a very simple method for a customer to identify weak areas in their environments:



For more findings, please refer to: https://www.threatdefence.com/why-threatdefence/our-findings/

About the author

Nick Theo is a ThreatDefence security engineer with an expert level background in Linux, AWS, Azure, Windows, DevOps and many other application and systems.

Nick is proficient in many scripting languages, is a certified Offensive Security Certified Professional with intimate knowledge on hacker techniques, tools and procedures.

This knowledge is translated into detection algorithms to help our customers do better than Tesla, Uber, Target and the Australian Defence Contractors.