
ASMGi
SafeBreach
Validate the Efficacy of Your Security Controls

ASMGi

SafeBreach

Can You Validate Your Security Controls In a WFH Environment?

Steven Roesing
Chief Executive Officer
ASMGi

Kimberly Becan
Director of Product Marketing
SafeBreach

Jay Bromberek
Regional Director
SafeBreach

April 16, 2020 | 1:00 pm to 2:00 pm EST | Webinar

Agenda

01

Validating Security Controls with SafeBreach

02

Top 5 Remote Workforce Risks

Email
Endpoint
VPN
Segmentation
Data Leakage

03

Demo

How to easily validate relevant security controls

Breach and Attack Simulation

For Security Control Validation

How do you provide value and efficacy of your security practice?

Breach and Attack Simulation - For Security Control Validation

Many Enterprises today …

- Implement security tools / technologies based on Frameworks (HIPAA, PCI, ISO 2700x, NIST, etc. = Controls-based)
- Don’t validate that the controls are working
- Don’t prioritize initiatives based on greatest risk to the organization
- Are not able to demonstrate return on investment AND reduction in risk

Breach and Attack Simulation - For Security Control Validation

What if there was a way to …


Get more from your existing security


Minimize security exposure


Ensure you are meeting compliance requirements


Test your Incident Response Plan


Prioritize initiatives based on actual Risk


Rationalize your cyber investments and demonstrate performance

ASMGi

Breach and Attack Simulation - For Security Control Validation

Online Poll

Do You Validate Security Controls?

1. **No**
2. **Yes, with annual Pen-Test**
3. **Yes, with RED TEAM exercises**
4. **Yes, with automated Breach Attack Simulation**

Reality of enterprise security

97%
of breaches are at companies which have already deployed the right controls

99%
of attacks are known and have been for years

95%
of firewall breaches are due to misconfiguration

Stop a Breach Before it happens

Validate your controls without the risk

Simulate TTPs to test your defenses

Visualize exposures with data-driven results

Holistically remediate to defend your enterprise

Proving the value and efficacy of your security practice

Simulate attacks

Safely and continuously run thousands of known threat indicators and attack behaviors to validate and improve your security controls.

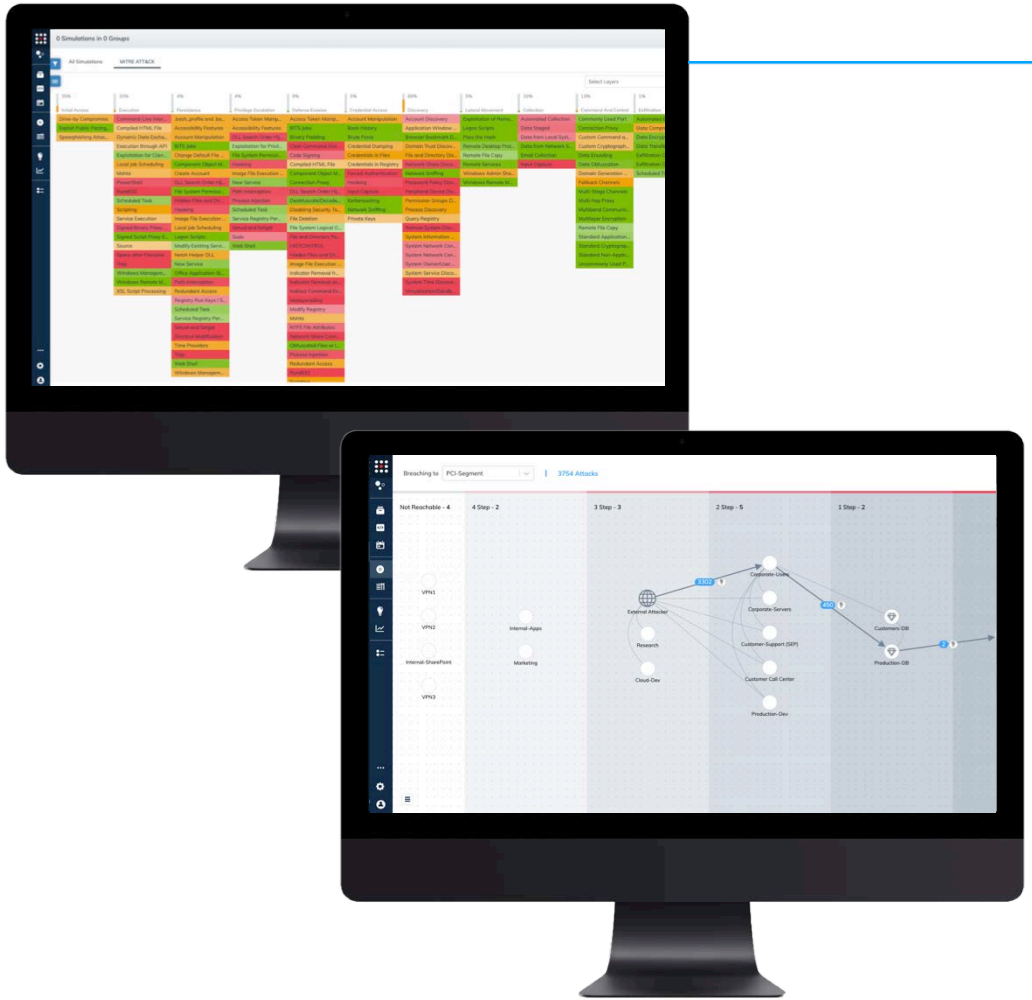
Content: 12,000+ Methods

Tactics, Techniques and Procedures

Malware Types

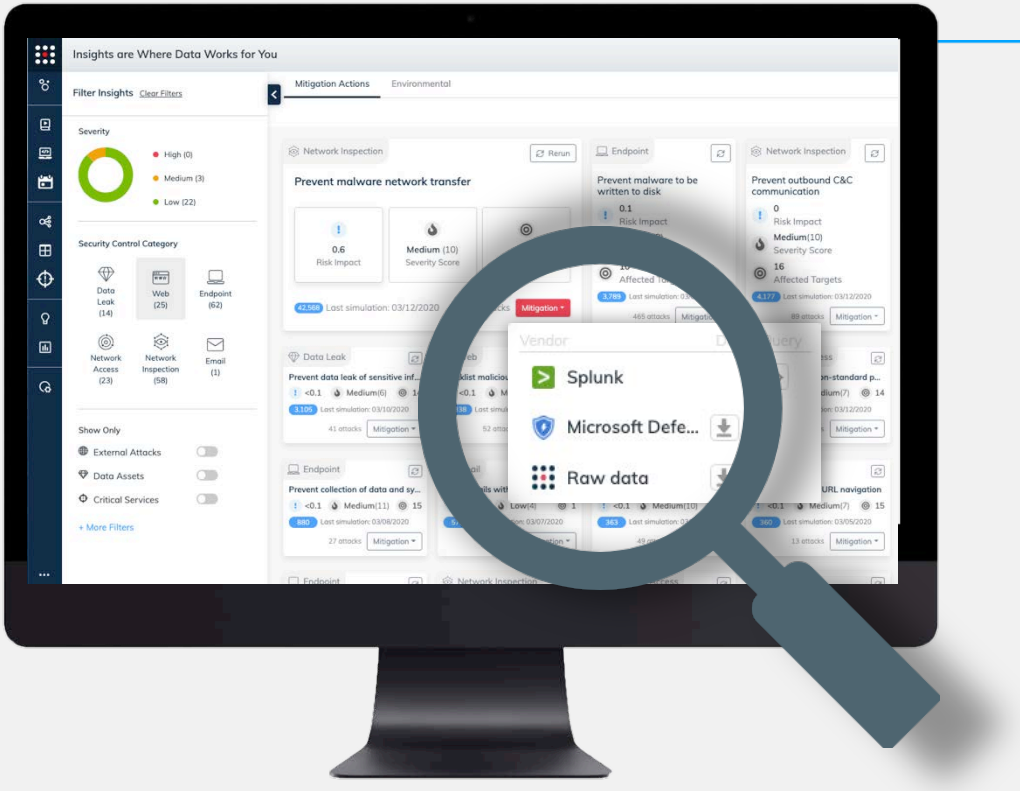
Custom Build Attacks

Threat Groups



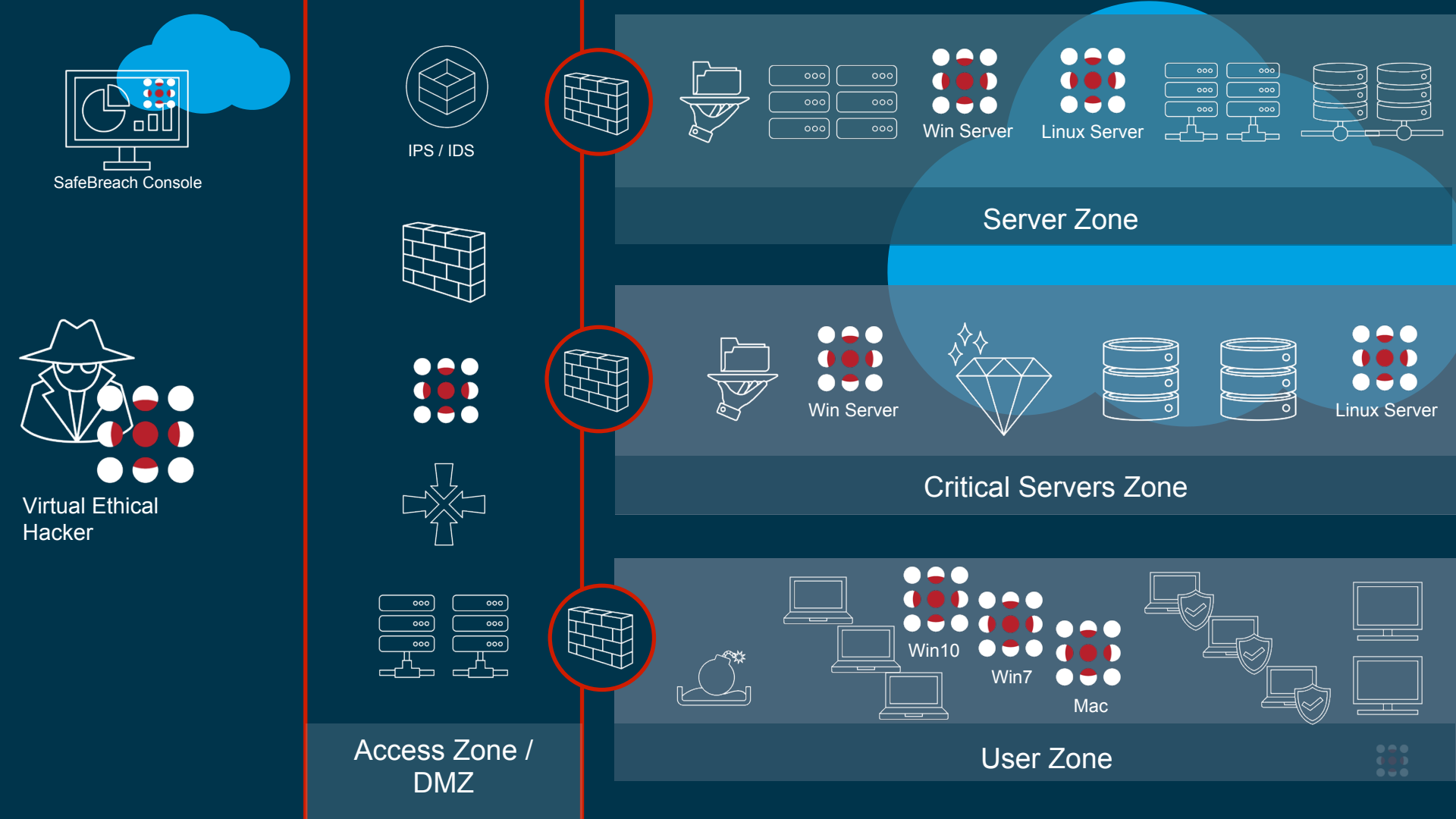
Visualize Your Posture

- MITRE ATT&CK Heat Map
- Risk Score
- Explorer View of Kill Chain
- Executive Reporting



Remediate Holistically

- Actionable prioritized remediation by business impact
- Aggregate and share remediation data to Network, Endpoint and SIEM solutions
- Ability to drill down to individual results for security control validation


SafeBreach Console
IPS / IDS
Win Server
Linux Server
Server Zone
Virtual Ethical Hacker
Win Server
Linux Server
Critical Servers Zone
Win10
Win7
Mac
Access Zone / DMZ
User Zone

Top 5 Security Validations for a Remote Workforce

ASMGi | SafeBreach

ZDNet CXO HARDWARE MICROSOFT STORAGE INNOVATION APPLE SECURITY MORE NEWSLETTERS ALL WRI

MUST READ: This new variant of Mirai botnet malware is targeting network-attached storage devices

A botnet is brute-forcing over 1.5 million RDP servers all over the world

Furthermore, statistics show that despite BlueKeep, most RDP attacks today are brute-force attempts.

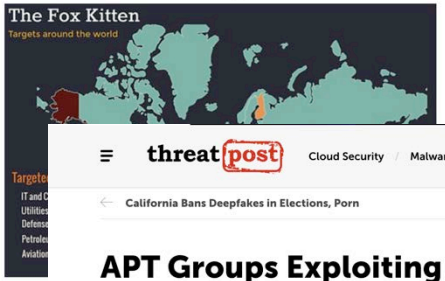
Fox Kitten – Widespread Iranian Espionage-Offensive Campaign

Posted on February 16, 2020 by ClearSky Research Team

During the last quarter of 2019, ClearSky research team has uncovered a widespread Iranian offensive campaign which we call "Fox Kitten Campaign"; this campaign is being conducted in the last three years against dozens of companies and organizations in Israel and around the world.

Read the full Report: Fox Kitten – Widespread Iranian Espionage-Offensive Campaign

Though the campaign, the attackers succeeded in gaining access and persistent foothold in the networks of numerous companies and organizations from the IT, Telecommunication, Oil and Gas, Aviation, Government, and Security sectors around the world.



ZDNet CXO HARDWARE MICROSOFT STORAGE INNOVATION APPLE SECURITY MORE NEWSLETTERS

MUST READ: This new variant of Mirai botnet malware is targeting network-attached storage devices

A Chinese APT is now going after Pulse Secure and Fortinet VPN servers

Security researchers spot Chinese state-sponsored hackers going after high-end enterprise VPN servers.

threatpost Cloud Security / Malware / Vulnerabilities / InfoSec Insider / Podcasts

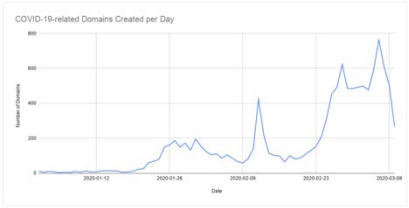
California Bans Deepfakes in Elections, Porn

APT Groups Exploiting Flaws in Unpatched VPNs, Officials Warn

Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide

MARCH 12, 2020 • INSIKT GROUP®

Insikt Group®



Graph showing the registrations of COVID-19-related domains per day in 2020. Recorded Future analysts created a query to find domain registrations of URLs containing "corona," "covid19," or "covid2019." Download the appendix for a list of these domains.

Official website of the Department of Homeland Security

CISA
CYBER+INFRASTRUCTURE

Search

About Us | Alerts and Tips | Resources | Industrial Control Systems | Report

National Cyber Awareness System > Alerts > COVID-19 Exploited by Malicious Cyber Actors

Alert (AA20-099A)

https://www.us-cert.gov/ncas/alerts/aa20-099a

COVID-19 Exploited by Malicious Cyber Actors

Original release date: April 08, 2020

Print | Tweet | Send | Share

Summary

This is a joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC).

This alert provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

Both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

APT groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails. This alert provides an overview of COVID-19-related malicious cyber activity and offers practical advice that individuals and organizations can follow to reduce the risk of being impacted. The IOCs provided within the accompanying .csv and .stix files of this alert are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this alert does not seek to catalogue all COVID-19-related malicious cyber activity. Individuals and organizations should remain alert to increased activity relating to COVID-19 and take proactive steps to protect themselves.

Technical Details

Phishing Email

Coronavirus disease (COVID-19) advice for the public - Messag

File Message Help Tell me what you want to do

HS

Thu 3/19/2020 8:41 AM

Healthcare System <ellistk@gmail.com>

Coronavirus disease (COVID-19) advice for the public

To [redacted]

Dear Families,

The Coronavirus (Covid-19) is wreaking havoc around the world. But if you know h

"Virus-Proof Your Life" you can prevent this invasive pathogen from getting past yo

natural defenses. developed using the latest, cutting edge research from major coll
and institutions across the globe.

Please go through this video and check what it's trying to tell you!

Thanks
Dr. Christopher Kawa, DC

P.S. : I've been in practice for almost 29 years and every day I'm researching the latest scientific evidence on heath so that I can teach my patients to function better and avoid disease. This special, one-of-a-kind e-book contains the latest, essential factors that lead to a strong immune system; one that can fight off bacteria and viruses with the God-given tools that we all have inside of us. I want to share this wisdom with you so that you and your family can all live happy, healthy lives.

COVID-19 Solidarity Response Fund for WHO - DONATE NOW

File Message Help Tell me what you want to do

WH

Sun 3/22/2020 5:41 AM

World Health Organization <COVID19Fund@fr.ocai.ch>

COVID-19 Solidarity Response Fund for WHO - DONATE NOW

To [redacted]

World Health Organization

We are all affected by the growing COVID-19 pandemic.
It's an unprecedented health challenge and we know people and organizations everywhere want to help.
The World Health Organization is leading and coordinating the global effort,
supporting countries to prevent, detect, and respond to the pandemic.

The greatest need right now is to help ensure all countries are prepared,
especially those with the weakest health systems.
Donations support WHOs work to track and understand the spread of the virus;
to ensure patients get the care they need and frontline workers get essential supplies and information;
and to accelerate efforts to develop vaccines, tests, and treatments.

See below for information on other ways to give, tax-deductibility and corporate and foundation giving options.

Now you can help us by donating any amount what you want help with the
BITCOIN NETWORK

Donate Now with Bitcoin payment.

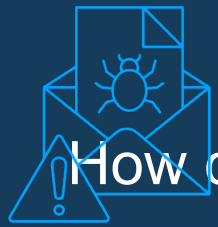
World Health Organization bitcoin address(BTC Wallet)for
donations:
16gmYrbqMr4SZeA7SqNVmirhnhDG3maYPK
Online donations made via bitcoin are tax deductible in the U.S. and Europe.
To the extent allowable by law.

The World Health Organization accepts checks or wire transfers from
anywhere in the world.
World Health Organization doesn't may to provide tax benefits to donors
to these payments.

Contact to email if you have any questions.

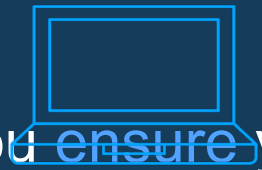
ASMGi

How can you ensure your extended remote workforce is secure?



Email

- Malicious Attachments
- Malicious Links
- Social Engineering



Endpoint

- Phishing Attacks
- Drive by Downloads
- Browser Exploits

VPNs

- Exploit VPN Vulnerabilities
- Brute Force Attacks
- Phishing VPN Credentials

Networks

- Brute Force Attacks
- Malware Propagation
- Remote Exploitation

Data Leakage

- Data Exfiltration
- Improper Permissions
- Unencrypted Communication

SafeBreach

DEMO

ASMGi | SafeBreach

Endpoint Controls

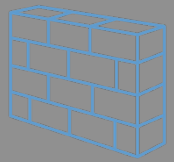
Relevant Attacker Techniques to watch

- **Infiltration techniques** - Monitor email and network for email, drive by and other download of malicious content
- **Host infection techniques** - file and fileless malware, malware execution
- **Host actions** - Monitor filesystem, registry and process dynamics for suspicious activities

VPN

Relevant Attacker Techniques to watch

- **Exploitation** - Monitor network activity for vulnerability exploitation attempts



Segmentation

Relevant Attacker Techniques to watch

- **Brute Force** - Monitor network activity for authentication attempts over common protocols internally available
- **Malware propagation** - Monitor network activity for the propagation of known malware
- **Remote Exploitation** - Monitor internal network activity for vulnerability exploitation and exploit delivery

Data Leak

Relevant Attacker Techniques to watch

- **Data Exfiltration** - Monitor network activity for sensitive content over a variety of protocols and channels
- **C&C Communication** - Monitor outbound communication for known C2 domains and C2 communication behavior

ASMGi | SafeBreach

Validate your Security Controls!

Top 5 Security Validations for a Remote Workforce

Contact ASMGi for more information:
sales@asmgi.com

Special Offer for Attendees

Q & A

Thank you!