

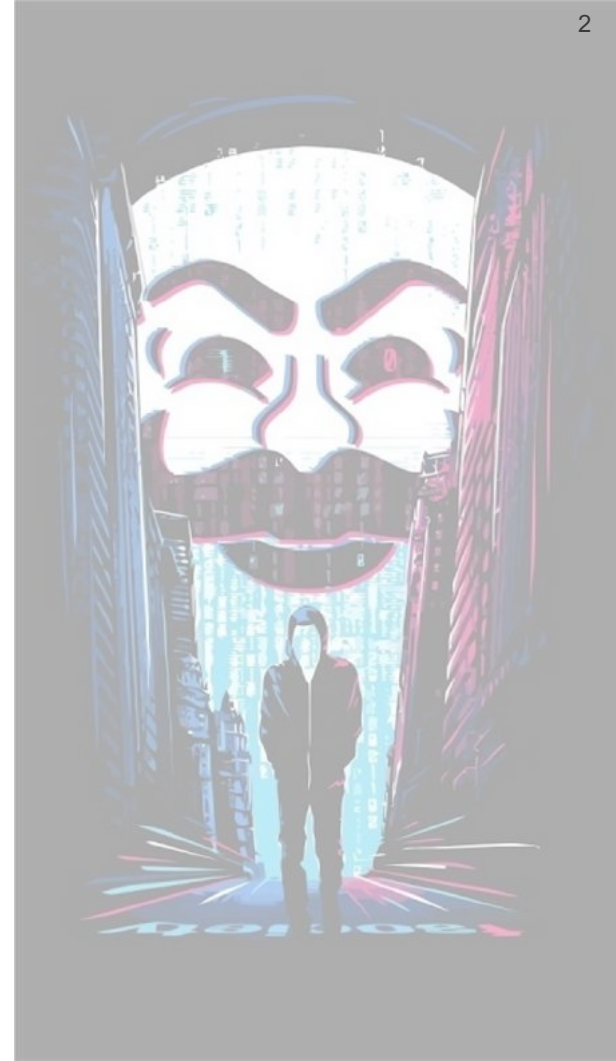


9 5222 4587 5437 EXP 03/15 0920 0502.5
ACCESS NO 4884 2943 21620 BALLAN
41 9876 681 EXP 06/16 4219 9761 6112 A
461 EXP 07/19 ACCT 4569 7701 2494 1344
1245 860 2475 ACCT 4461 7641 9110
7 4200 3771 4045 00 ACCT 8864 3145 34
156 29 EXP 07/83 5434 976 BALANCE DUE
156 29 EXP 07/83 5434 976 BALANCE DUE
41 9876 681 EXP 06/16 4219 976
3 BALANCE DUE 1214 9467 1101 3487 EX
4200 3771 4045 00 ACCT 8864 3145 34
156 29 EXP 07/83 5434 976 BALANCE DUE
RRP PAYE BALANCE 0934 4892 2591 58
4 2943 21620 BALLANCE DUE 0881232 7
ACCT 4461 7641 9110 3641 33 1640
ACCT 4461 7641 9110 3641 33 1640
85 2365 1476 BALANCE DUE 9084 2245
7 359 134 EXP 4/18 1956 2387 4561 445
2222 4587 5137 EXP 03/15 0920 0502 01
ACCESS NO 4884 2943 21620 BALLANCE
98876 661 EXP 06/16 4219 9761 6112 A
EXP 07/19 ACCT 4569 7701 2494 1344
BALANCE DUE 1214 9467 1101 3487 EXP
156 29 EXP 07/83 5434 976 BALANCE DUE
29 EXP 07/83 5434 976 BALANCE DUE
ACCESS NO 4884 2943 21620 BALLANCE
3461 EXP 07/19 ACCT 4569 7701 24
1245 860 2475 ACCT 4461 7641 9110
2110 3487 7704 ACCT 8414 2214 1452 2
06/16 01287 41789 2385 1476 BALANCE
8468 235 3696 7368 134 EXP 4/18 1956
ESS 01 1214 ACCESS NO 4884 2943 216
16 6446 0 6562 3461 EXP 07/19 ACCT 456
7633 20 9754 1245 680 2475 ACCT 446

Mr. Reality or Mr. Robot?

Michael Haas – Area Sales Director Central Europe

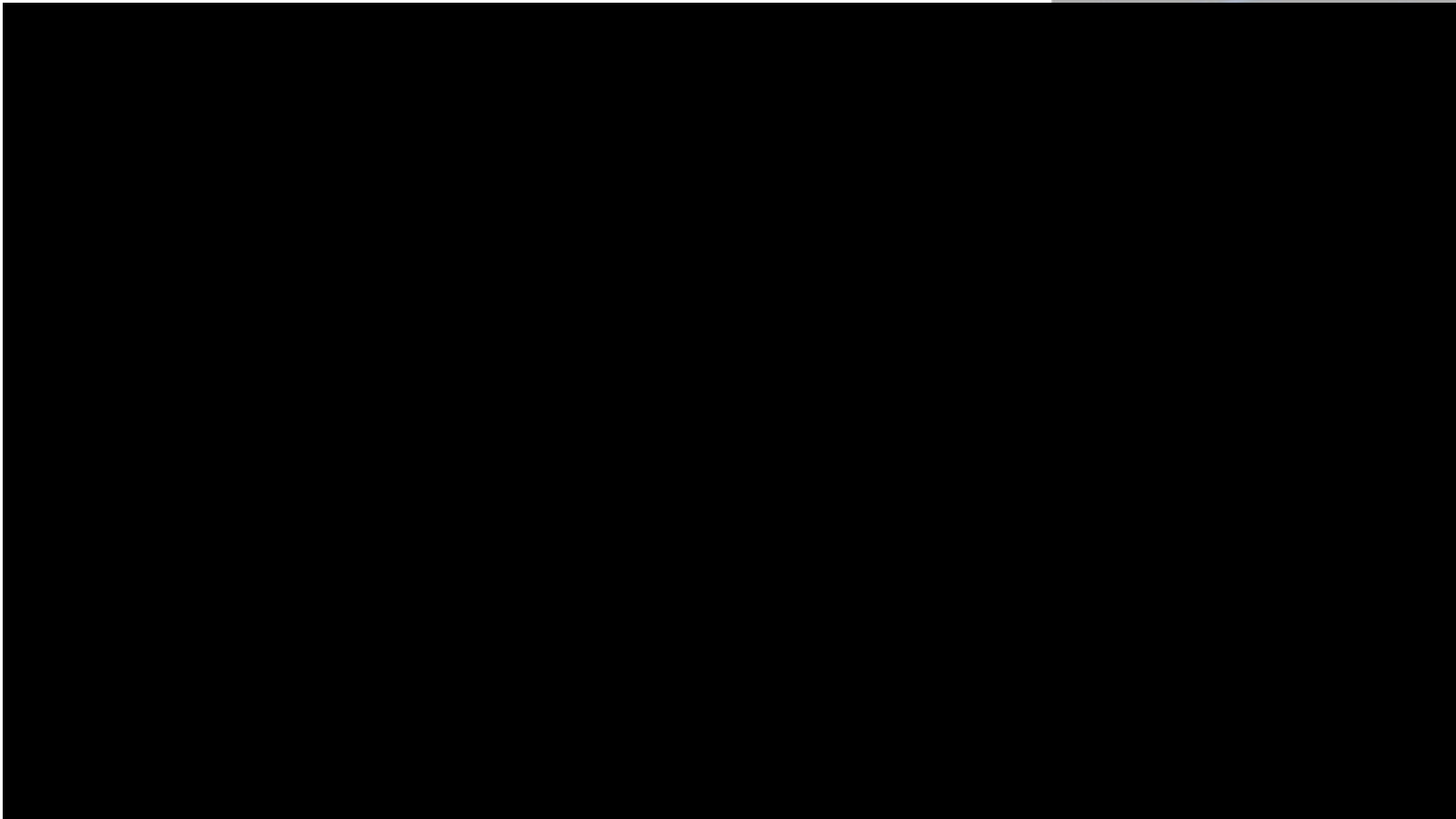
Umfrage 1



Agenda

- **Quick Look at Hollywood Hacking**
 - And why Mr. Robot is better
- **Five Real Threats from Mr. Robot**
 - Top threats to beware
 - Mr. Robot examples vs real world
 - Corresponding defenses
- **Summarizing Defense**

Hollywood



A close-up, high-contrast photograph of a man wearing a dark hoodie, looking directly at the camera with a serious expression. The lighting is dramatic, highlighting his face against a dark background.

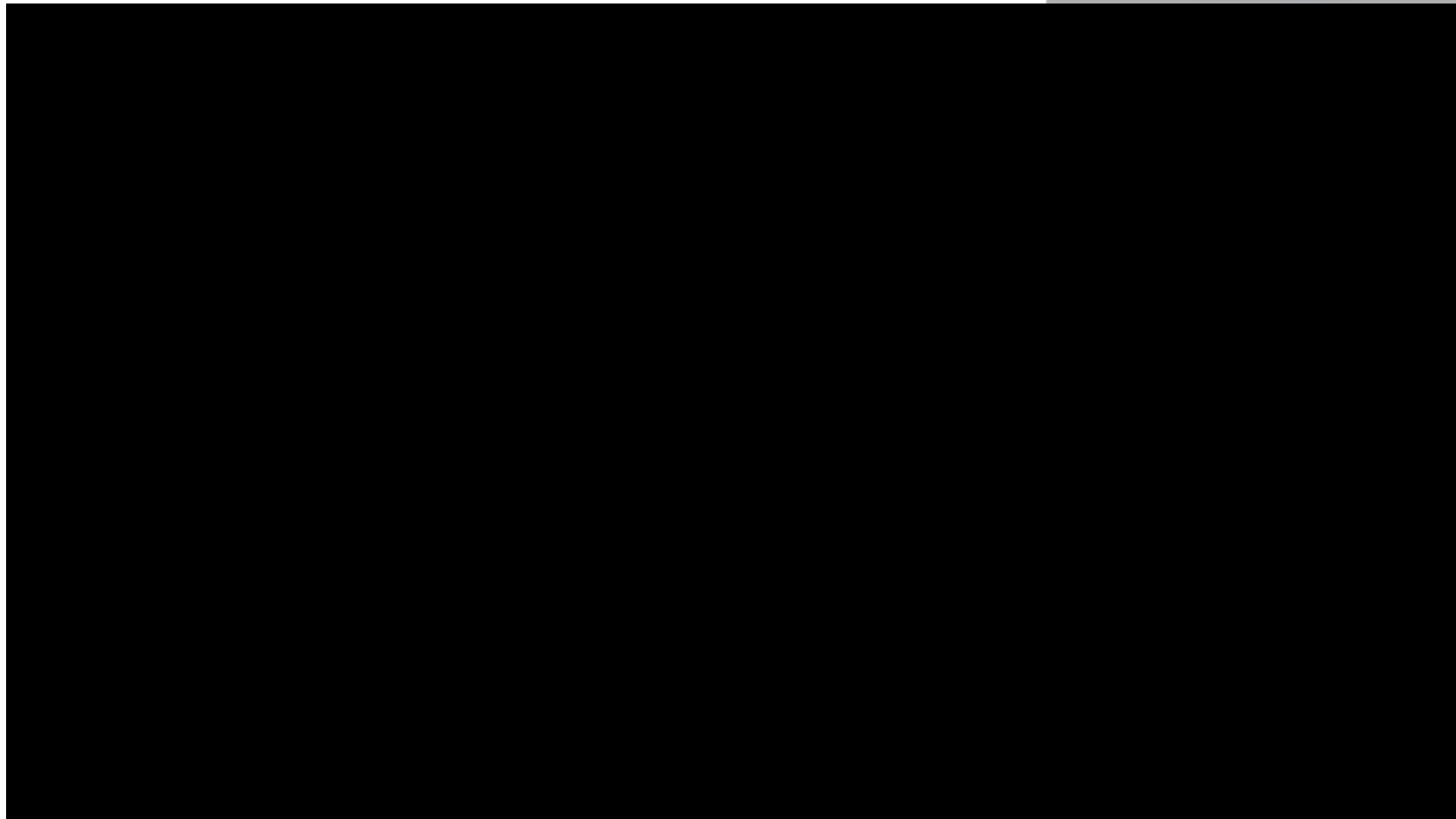
**5 Real-World
Threats
from**

MR. ROBOT

Video 1



Video 2 – Theme #1



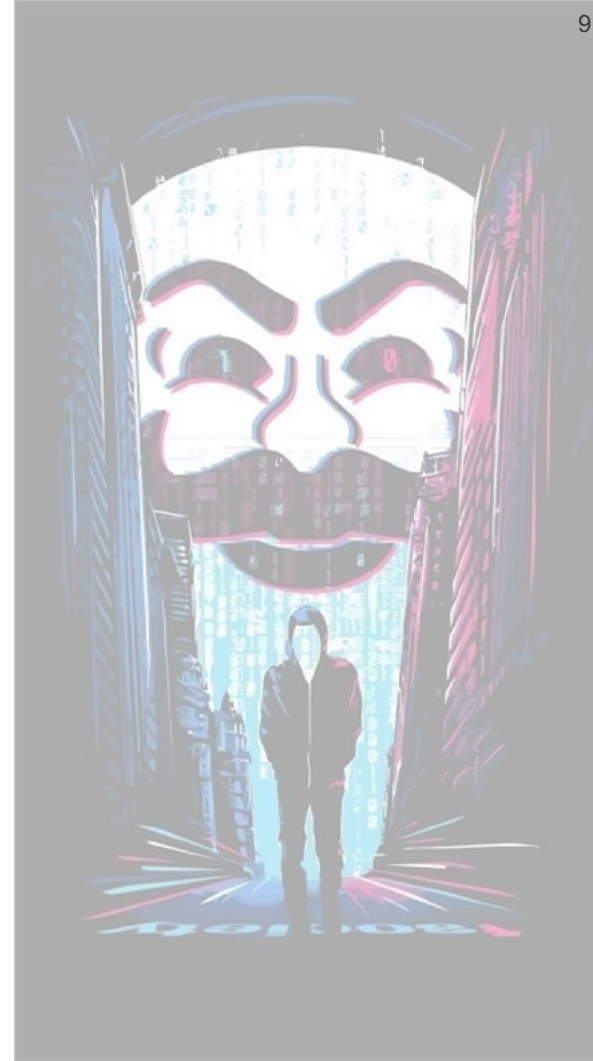
Theme #1: Phishing

Real-World

- **80%** of malware is delivered by phishing – *Threatsim*
- **91%** of targeted attacks start with SPEAR-phishing – *Trend Micro*
- **76%** of organizations reported being victim of a phishing attack in 2016 - *Wombat Security*

Mr. Robot

- Elliot phishes Shayla passwords
- FBI tries to phish Elliot
 - Elliot also reverse phished the FBI



Flavors of Phishing

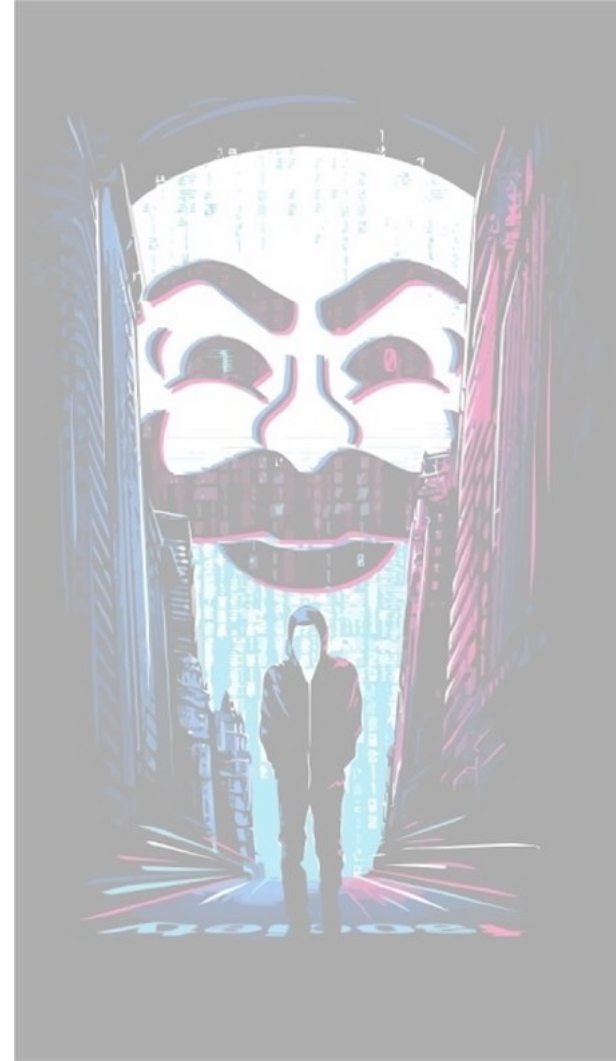
Phishing — luring a victim into giving up credentials or doing something via a legitimate seeming email

Spear-phishing — A more customized phishing email that targets a specific individual or group

Whaling — spear-phishing that targets C-levels

Old phishing example:

- Not individualized
- Bulk recipients
- Uses real assets
- Malicious document

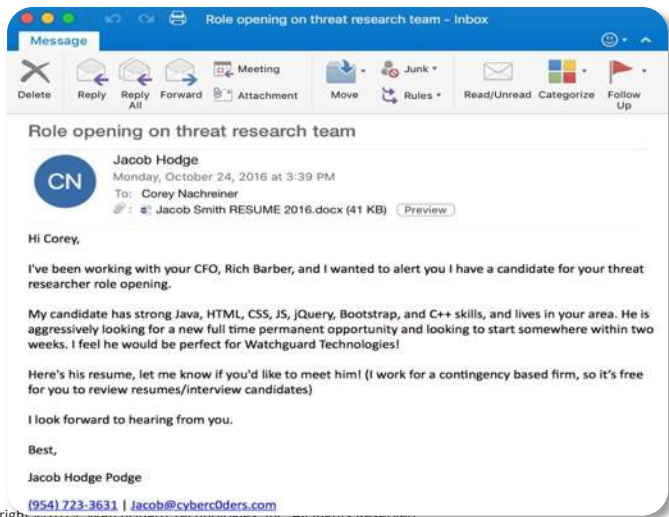
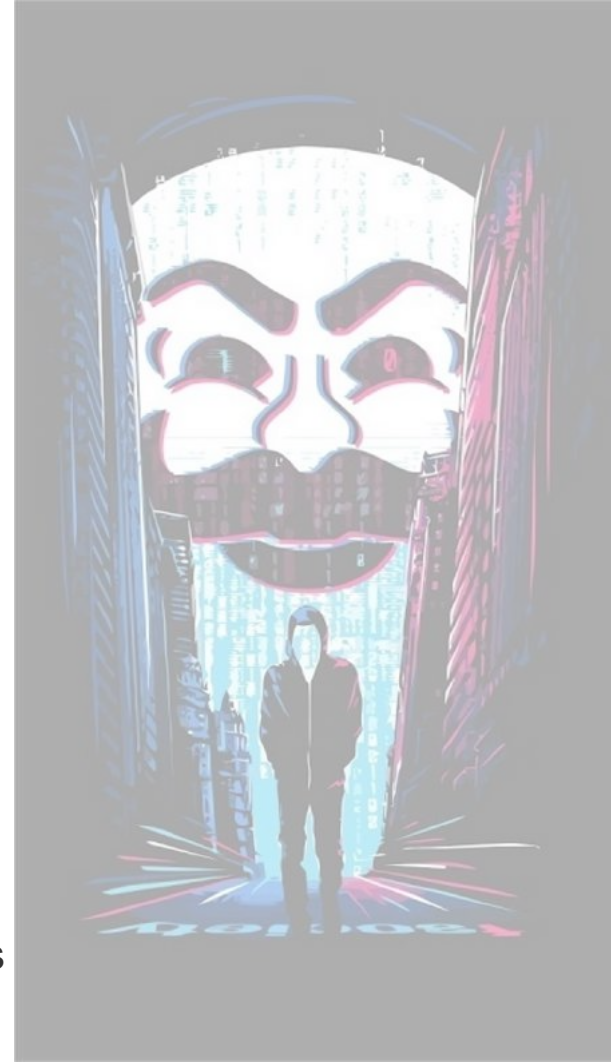


Flavors of Phishing

Phishing — luring a victim into giving up credentials or doing something via a legitimate seeming email

Spear-phishing — A more customized phishing email that targets a specific individual or group

Whaling — spear-phishing that targets C-levels



Spear-phishing example:

- Personalized to me
- Fits my job role
- Understands business relationships
- Sender makes sense in context
- Malicious attachment fits context

Users Still Click Phishing Emails

From: john.smith@turner.com

To: zinaida.benenson@fau.de

Subject: CNN request -- about your upcoming Black Hat talk

7

Zinaida,

John at CNN here. I'm the news network's cybersecurity reporter. [Here's a link to my work](#), in case you're not familiar with it.

I saw the description of your upcoming Black Hat talk. Your topic looks fantastic!

Can we get an exclusive look at your talk?

Cheers,

John Smith

john.smith@CNN.com

50%

0%

Study 1: a
clicked

and yet they click

From: Journal of Experiments (EXPE) exp@editorial-expe.com

To: zinaida.benenson@fau.de

Subject: Invitation to Peer Review EXPE-M-35-00737

Dear Dr. Benenson, In view of your expertise [...]

[...]

If you would like to review this paper, please click this link:

<http://expe.editorial-expe.com/l.asp?i=35189&l=GKXKMQK>

If you do not wish to review this paper, please click this link:

<http://expe.editorial-expe.com/l.asp?i=87665&l=6HN7KK>

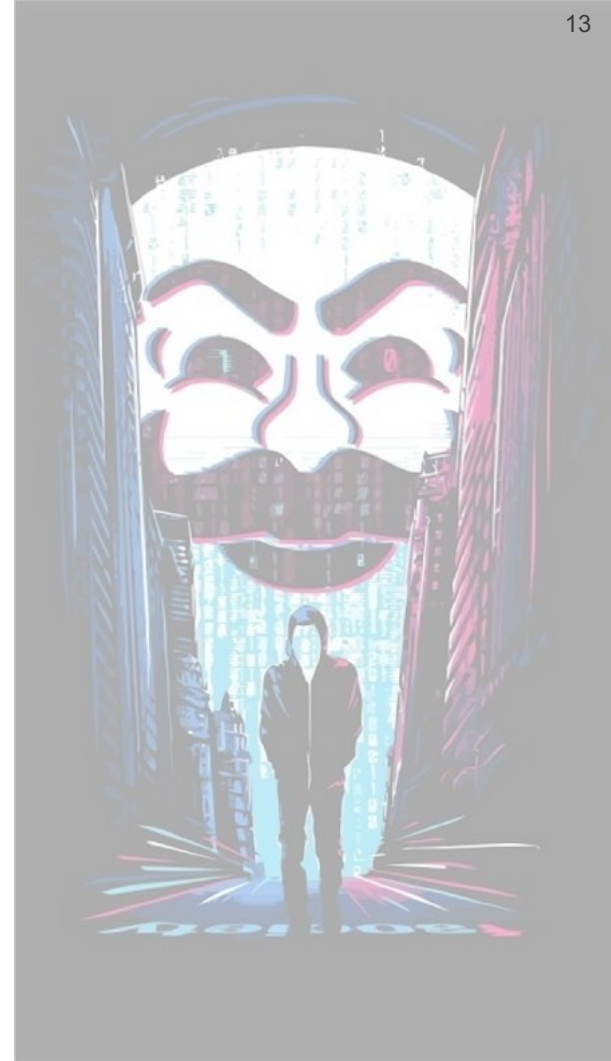
Best regards,

Editor

<name I've never heard of>



Umfrage 2

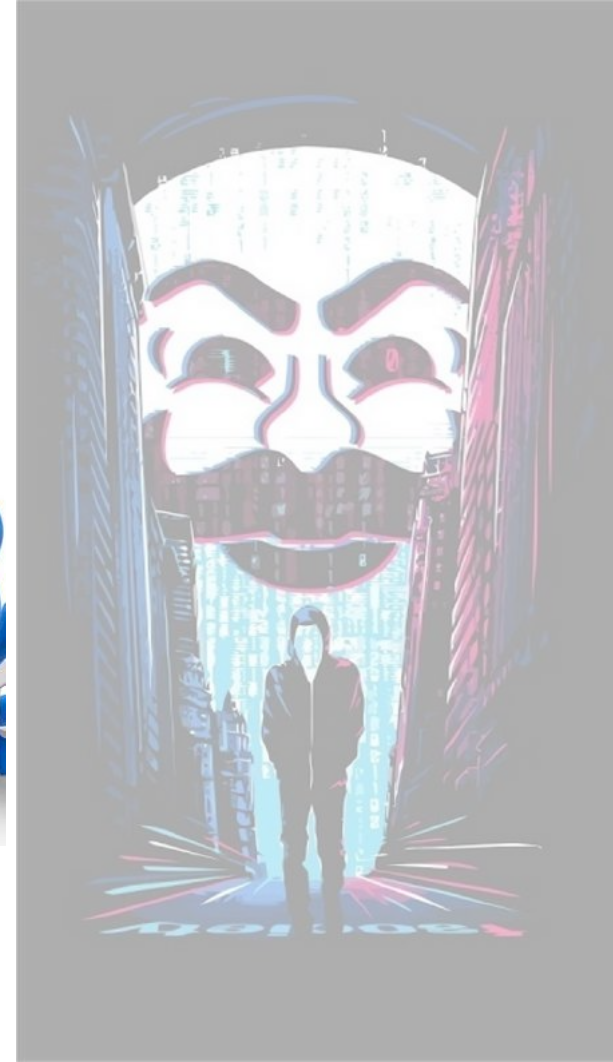


Prevention: DNS Blocking & Awareness Training

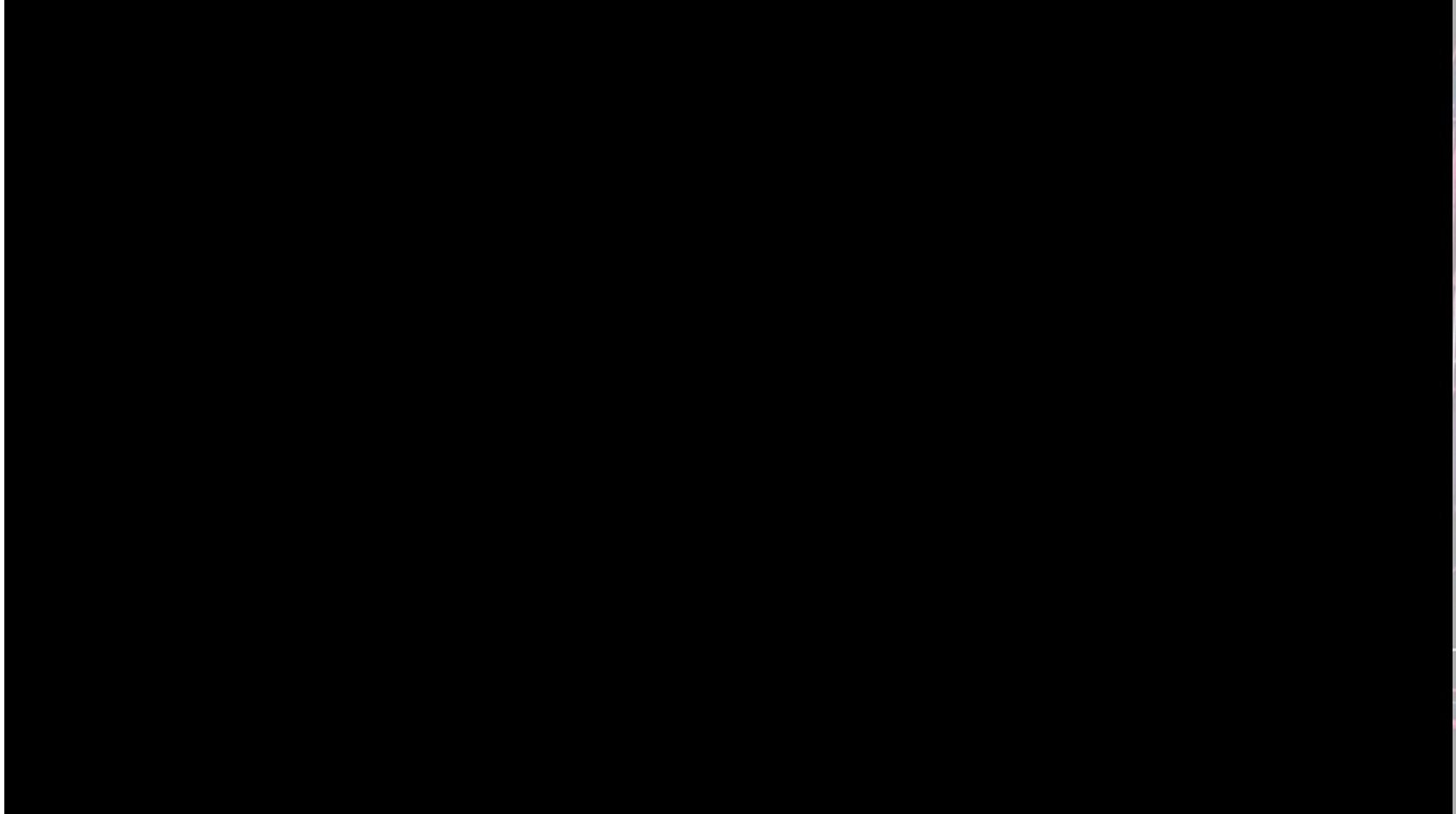
Link filtering



Focus on phishing training



Video 3 – Theme #2



Theme #2: Ransomware

Real-World

- Ransomware was top payload 2016/2017
- Estimated to cost \$5 Billion in loses (2017)
- WannaCry the first RansomWORM

Mr. Robot

- Darlene uses Social Engineers Toolkit (SET) to create infected USB
- Ransomware looks very much like Cryptowall
- Jester: a popular real-world hacker

```
3. RATTE (Remote Administration Tool Tommy Edition) Create Payload
me/RATTE-Reademe.txt first

99) Exit the Social-Engineer Toolkit

set:modules> 1
set:modules:webattack> Enter IP address:: 192.251.68.254
set:modules:webattack> Enter Port [80]: 80
set:modules:webattack> Cryptowall recursive attack to all computer
set:modules:webattack> Type the name of the attack file: cryptowall
set:modules:webattack> Enter secret key passphrase: *****
[-] preparing fsociety Cryptowall_
[*] Payload has been exported to /root/.set/fsocietyM.exe
set:modules:webattack> Create autorun.inf [yes|no]: yes
[-] Autorun.inf has been exported to %s/autorun.inf
[-] Copy %s/autorun.inf and %s/fsocietyM.exe to /media/root/FLASH
[-] Payload completed! Good Luck
```



Ransomware Hitting State and Local

Baltimore city government computer network hit by ransomware attack

S By IAN DUNCAN and COLIN CAMPBELL
THE BALTIMORE SUN | MAY 07, 2019 | 6:50 PM

The Baltimore City government computer network is infected with ransomware.



Baltimore city government computers were infected with ransomware Tuesday, the mayor's office said, the second time in just over a year that hackers demanding payment disrupted the city's technology systems.

"Employees are working diligently to locate the source and extent of the infection," said Lester Davis, a spokesman for Democratic Mayor Bernard C. "Jack" Young.

[More: Ransomware attack on Baltimore government computers 'very serious issue' »](#)

Davis said critical systems, including 911 and 311, were not been affected, but that the majority of city servers were shut down. The effects ranged from a City Council committee canceling a hearing on gun violence to water customers being unable to get billing questions answered.

The New York Times

Ransomware Attack Hits 22 Texas Towns, Authorities Say

The state declined to say which towns were affected by the coordinated cyberattack. But one expert said it could signal more such attacks in the future.



Prevention: Advanced Malware Detection

The most advanced malware protection on the market

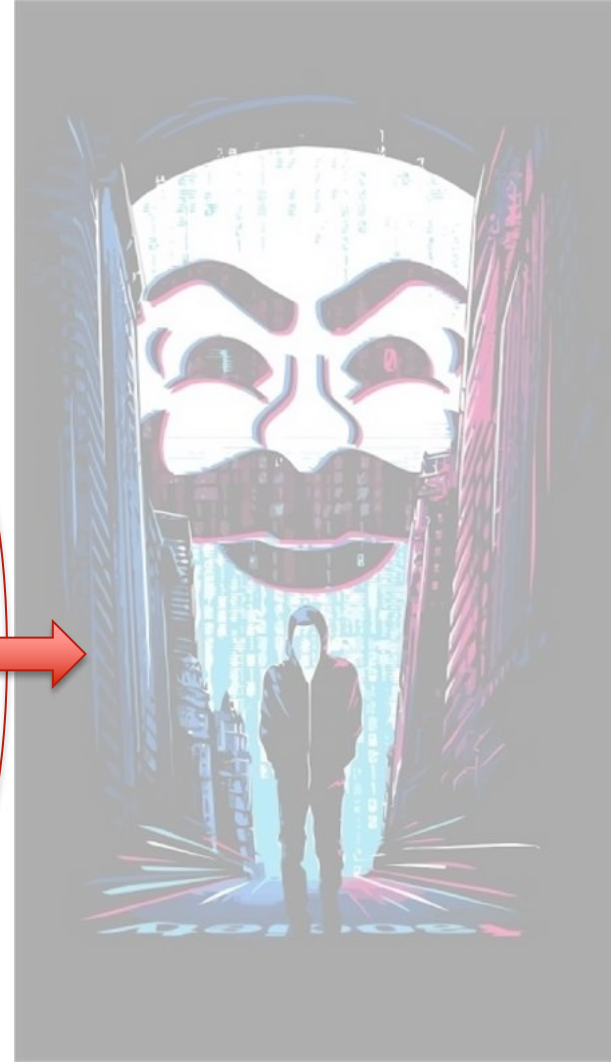
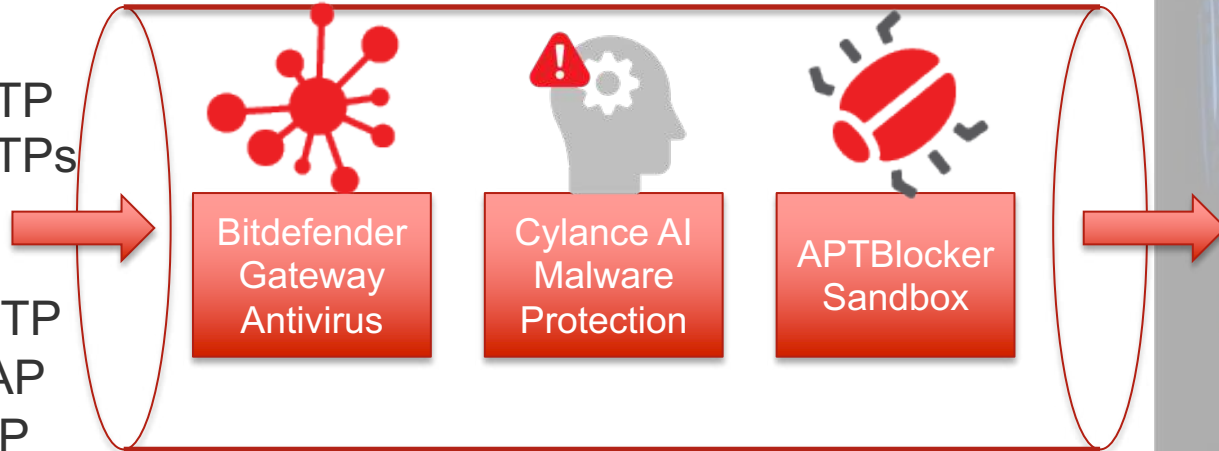
Web

- HTTP
- HTTPS

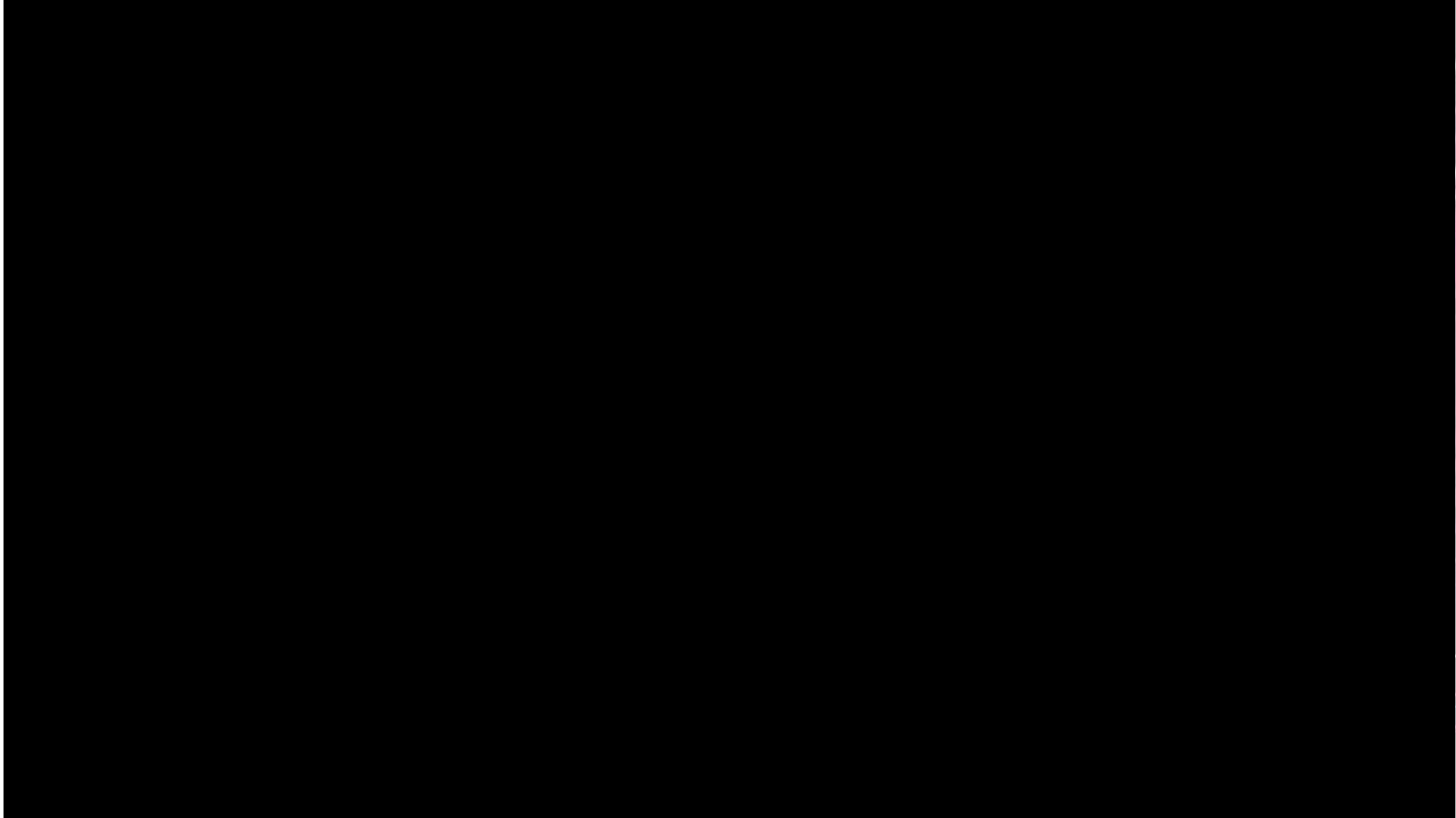
Email

- SMTP
- IMAP
- POP

Others...



Video 4 – Theme #3



Theme #3: IoT Attacks

Real-World

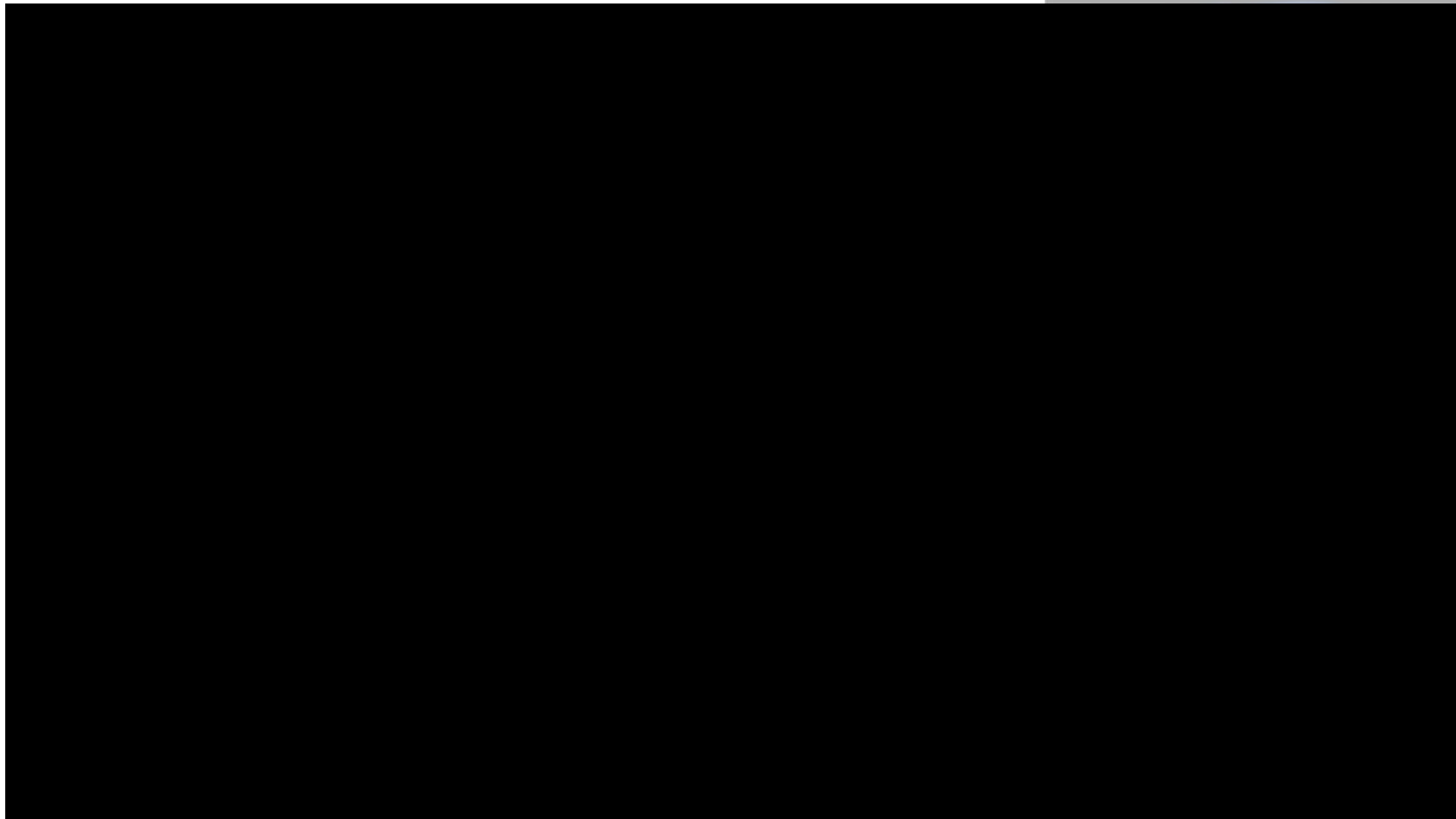
- Mirai Botnet infected > 300K devices
- Created record 1Tbps DDoS Attacks
- Devices from kids toys to home automation hacked

Mr. Robot

- Hack started with the wearable (Bluetooth?)
- Entered password twice... Accel tracking?
- No tech detail, but theoretical accurate result of home automation hack
- *Did you spot the hacker?*



Video 5



IoT Attacks Build Off Mirai

Krebs on Security
In-depth security news and investigation

21 KrebsOnSecurity Hit With Record DDoS

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at Akamai, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

My New Book!

SPAM NATION
NEW YORK TIMES BESTSELLER
THE INSIDE STORY OF CREATED CYBERSPY-FROM GLOBAL SPYING TO YOUR FRONT DOOR
BRIAN KREBS

Krebs hit with 620Gbps DDoS

The Hacker News
Security in a serious way

+1,474,344 304,322 1,475,095

World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices

1 Tbps DDoS Attack
Powered By 150,000 Hacked IoT Devices

Do you know - Your Smart Devices are the new cyber attack that Internet has just witnessed.

TRENDING STORIES

- Massive DDoS Attack Against Dyn DNS Service Knocks Popular Sites Offline
- An Army of Million Hacked IoT Devices Almost Broke the Internet Today
- Dirty COW - Critical Linux Kernel Flaw Being Exploited in the Wild
- Massive ATM Hack Hits 3.2 Million Indian Debit Cards - Change Your PIN Now!

OVH hit with 1Tbps DDoS

IoT DDoS targets DNS

Mass internet disruption caused by DDoS attack on DNS company Dyn (update)

PAUL SAWERS - OCTOBER 21, 2016 7:25 AM

TAGS: CYBERSECURITY, DDoS, DDoS ATTACK, DNS, HACKING, SECURITY

Above: Datacenter / Server Room
Image Credit: Shutterstock

A major cyberattack affected hundreds of websites today, including the *New York Times*, Reddit, Twitter, Spotify, and eBay.

The attack actually centered on Dyn, a New Hampshire-based company that offers a platform to optimize websites' online performance. This includes monitoring and controlling applications and infrastructure with data and analytics to reduce traffic and ensure end-users aren't impacted by slow response times.

Dyn's DNS service acts as a bridge between human-readable domain names and IP addresses that the internet is able to understand, and it was customers of this managed DNS service that were impacted. The distributed denial-of-service

DARKRe

Analytics Attacks / Breaches AppSec Careers / Cloud Endpoint IoT Mobile Operations Penmeter Risk Threat Intelligence Vulnerabilities / Threats

VULNERABILITIES / THREATS

7 Variants (So Far) of Mirai

Mirai is an example of the newest trend in rapidly evolving, constantly improving malware. These seven variants show how threat actors are making bad malware worse.

Change, as we know, is the only constant. Malware - which is evolving rapidly sprouting new features and functionality, and becoming more difficult to find and eradicate - is no exception to the rule.

One of the most notable examples is Mirai, botnet malware first described in August 2016. Mirai quickly won notoriety as the engine for some of the largest DDoS attacks seen to date.

Ever since Mirai's author, a hacker going by the handle Anna-Sempai, released the malware's source code less than two years ago, the malware community has been enthusiastically developing new variants. Some change specific IoT devices, some change the purpose of the bot, some combine Mirai with other malware families, and some add new capabilities and functionality. With every new variant, the legacy of Mirai is extended.

With agile discipline spreading to malware, it is useful to look at the evolution of Mirai as an example of what could happen to other malware families. While

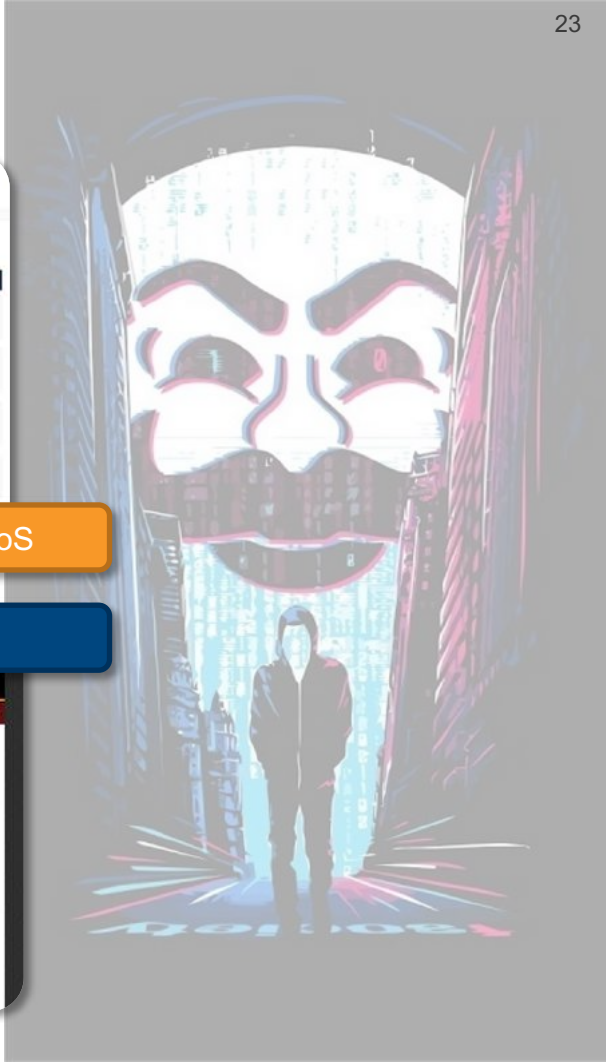
EDITOR'S CHOICE

- 12 Free, Ready-to-Use Security Tools
- Most IT Security Pros Want to Change Jobs
- Most Malware Arrives Via Email

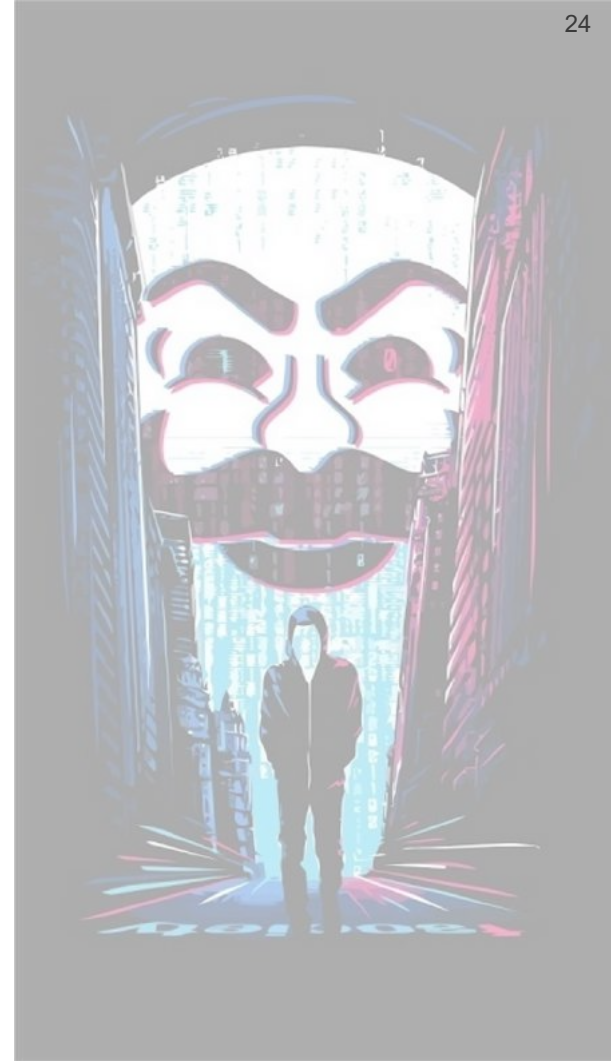
SUBSCRIBE TO NEWSLETTERS

WEBINARS

SOX Evolution: How and Why to Update Your Security Operations Center



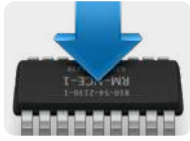
Umfrage 3



Prevention: IoT Defense



Security by **Design**



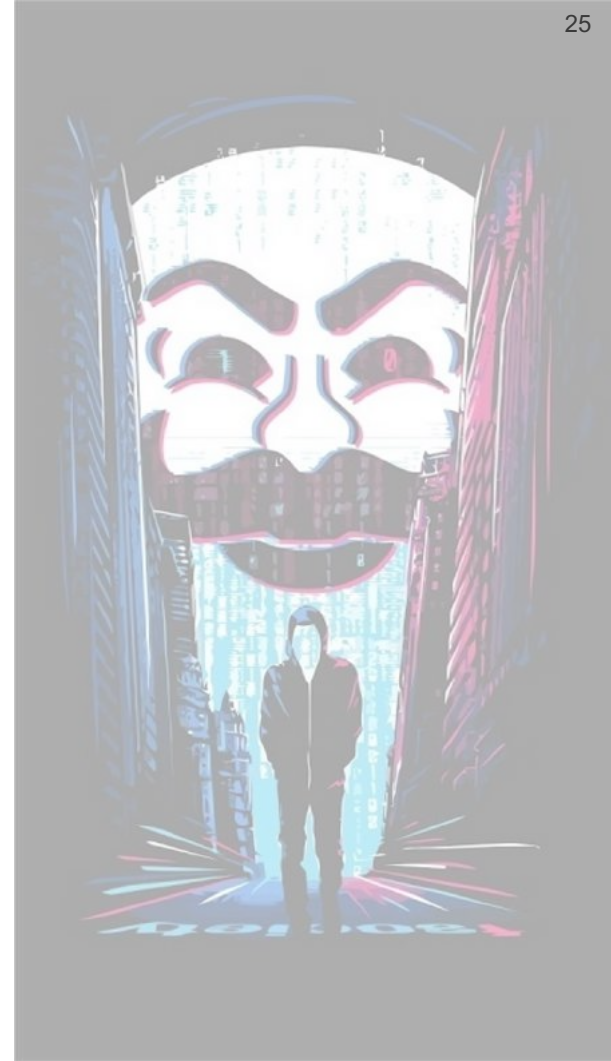
Firmware needs updates too



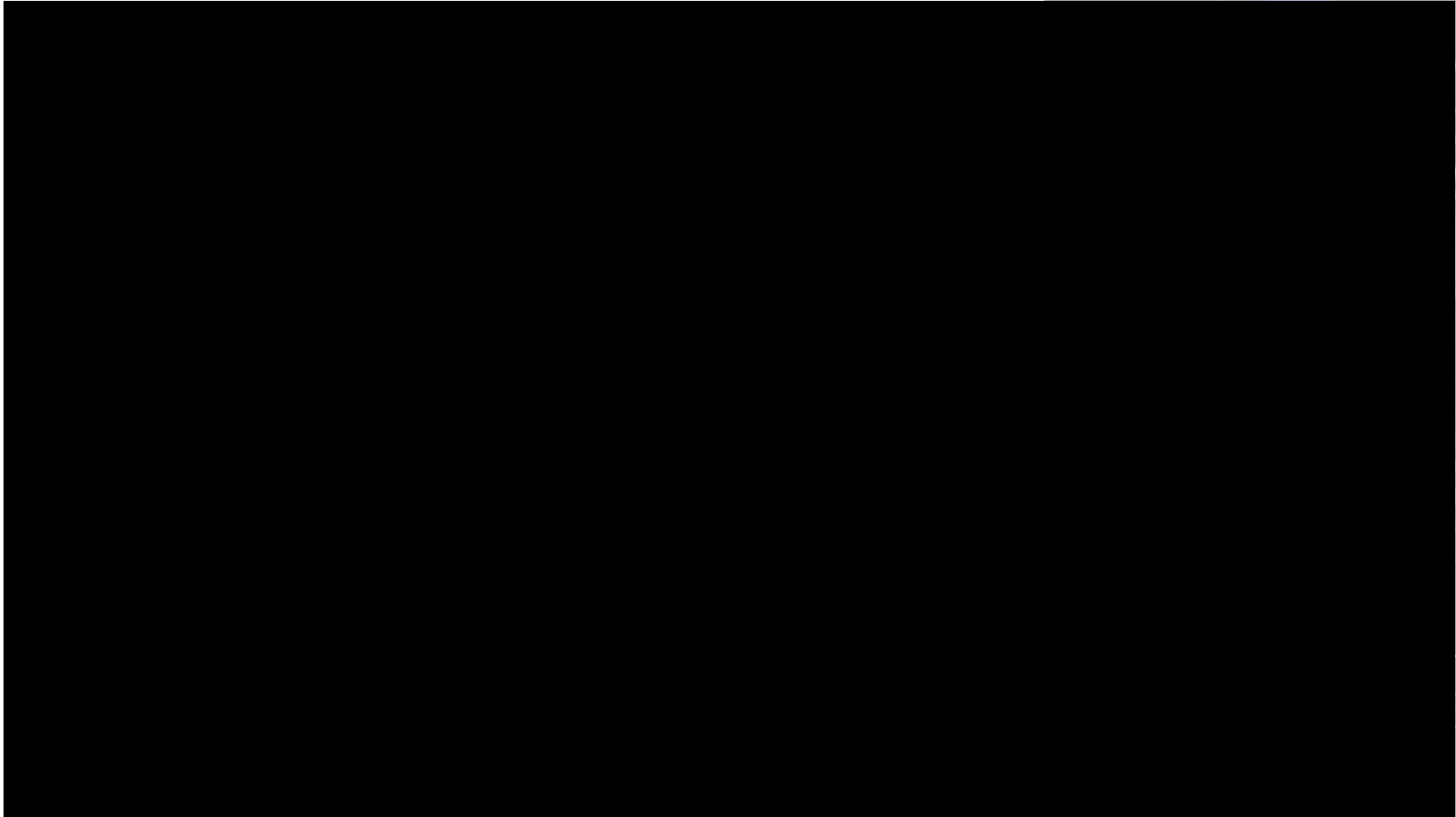
Network protection is **device agnostic**



Segment your IoT equipment



Video 7 – Theme #4



Theme #4: Wireless Hacks

Wireless hacks are real: Hotel Wi-Fi Hacking



- Attacker sits by pool with a Pineapple
- Copies hotel's real Wi-Fi
- Guests phones/tablets auto-connect
- Attacker sees/steals in real time:
 - Credit card number
 - Flight itinerary
 - Email address and password
- Leaving no trace behind

Read story at Secplicity.org:



Wi-Fi Hacking at the Hotel Pool



Russian Evil Twin Attacks



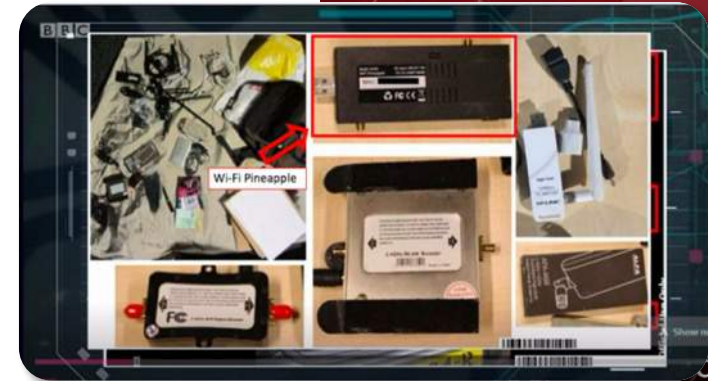
Russian Wi-Fi Hacking – Evil Twin attacks EXPLAINED

October 7, 2018 By Ryan Orsi

News broke this week highlighting the use of a nearly two-decade old Wi-Fi hacking technique called an Evil Twin attack. Despite being a known attack vector, Evil Twin attacks remain difficult to prevent without the proper protections in place. In the following article, we'll detail how Russian hackers used this technique to infiltrate Wi-Fi networks, and how to defend against attacks like this.

Wi-Fi Spies Caught

The US Department of Justice charged hackers within the Russian military agency, GRU, with



Prevention: WatchGuard Wi-Fi WIPS

Table 1: Test Results per Vendor

Test	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
	Detect	Prevent	Detect	Prevent	Detect	Prevent	Detect	Prevent
Rogue AP	P	P	F	N/A	F	MP	F	N/A
Rogue Client	P	P	F	N/A	F	MP	N/A	MP
Neighbor AP	P	P	P	P	F	N/A	F	N/A
Ad-Hoc Network	P	P	F	N/A	F	N/A	P	N/A
"Evil Twin" AP	P	P	P	F	P	MP	P	F
Misconfigured AP	P	P	P	N/A	N/A	N/A	N/A	N/A
Concurrent Threats	P	P	F	F	F	F	F	F

P – Pass

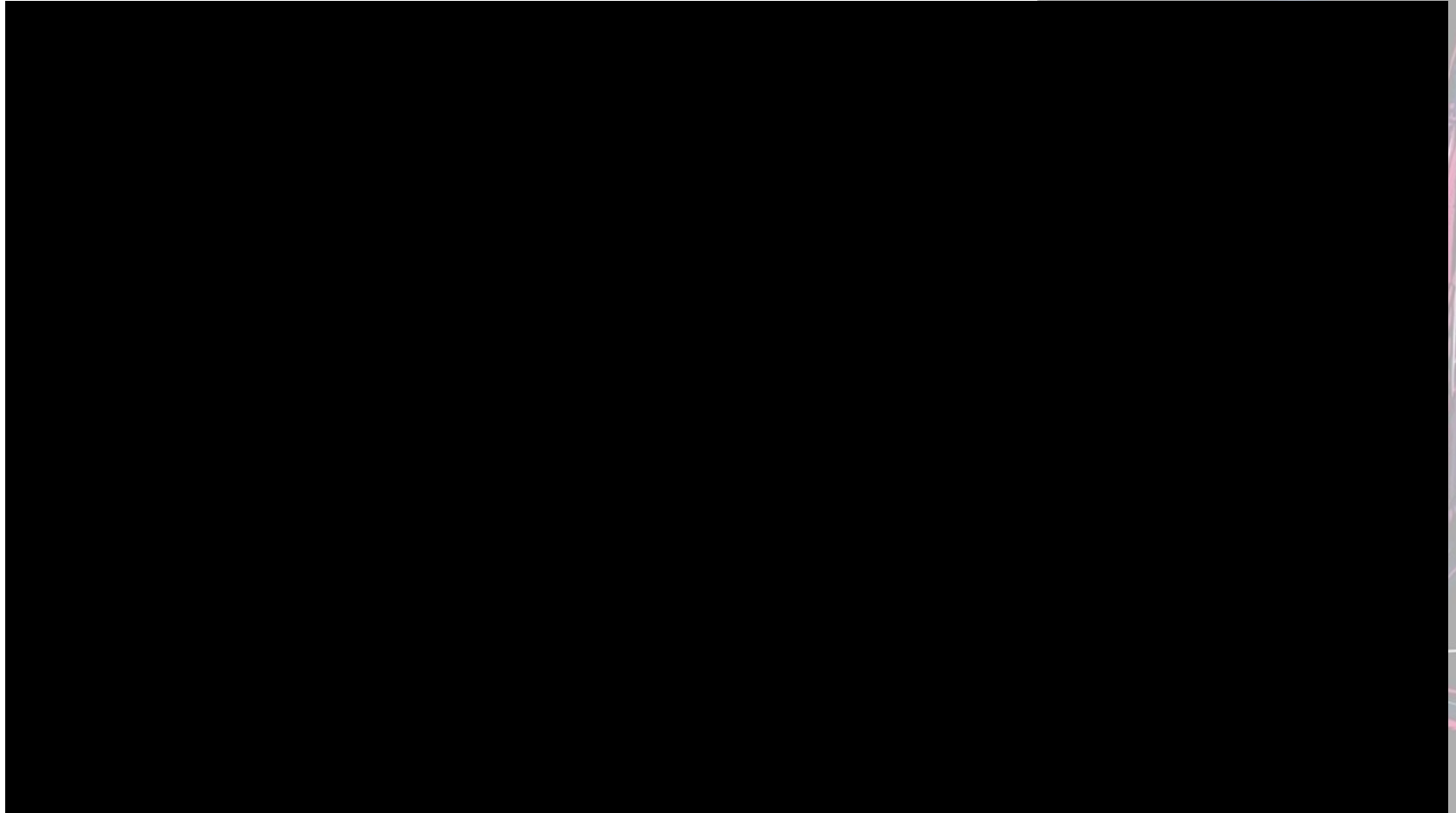
MP – Marginal Pass; require manual prevention

F – Failure to detect or protect from the referenced test

N/A – Feature not supported



Video 8 – Theme #4



Theme #5: Authentication Attacks

Collection of 1.4 Billion Plain-Text Leaked Passwords Found Circulating Online

Monday, December 11, 2017

Tweet Share LinkedIn

hackers always first go for the weakest

23 MAR 2017 NEWS

Home Depot to Pay \$27.25m in Latest Data Breach Settlement

Tara Seals US/North America
Email Tara

In the latest settlement with Home Depot, the retailer has agreed to pay \$27.25 million to settle a lawsuit filed by a consumer group. Illustrating the real-world consequences of a data breach, the settlement is ultimately good for consumers, but it's much more once legal fees are taken into account. The 2014 incident, which involved a credit-card compromise, was the first time that a retailer filed a valid claim with a court, even if they have to pay their losses. This may get an idea of how much more once legal fees are taken into account.

PARASITES

Hackers Are Using Uber's 57 Million Account Data Breach to Steal Passwords

Even if Uber's stolen database of account details seemingly isn't being traded on the digital underground, hackers are using it to steal customer's passwords.

JOSEPH COX 11:23:47 8:41 AM ET

Where there's a data breach, there's a way to exploit it. If you don't have access to the realm of the stolen data, you can't exploit it.

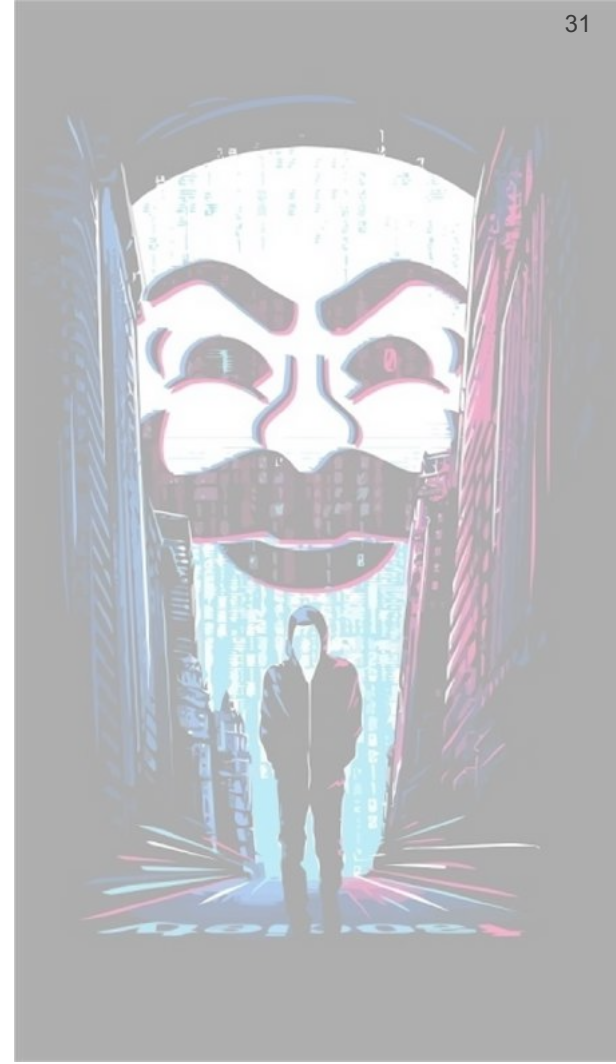
On Tuesday [Bloomberg reported](#) that in a 2016 breach of 57 million account details, hackers stole the phone numbers of 50 million ride-sharing users. [New news](#) by sending potential Uber users their passwords to steal their password.

BITCOIN: \$64m in cryptocurrency stolen in 'sophisticated' hack, exchange says

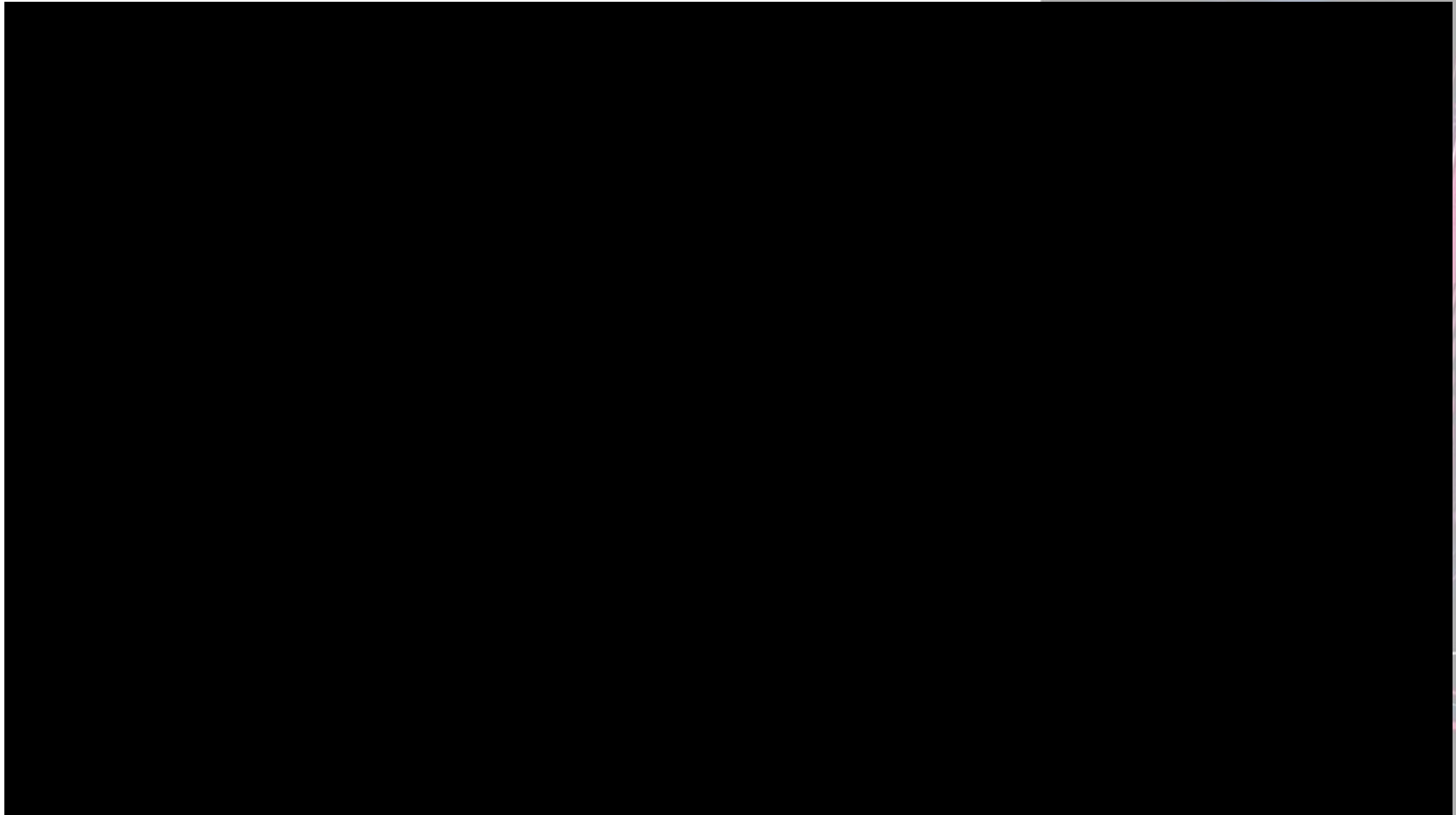
Bitcoin marketplace NiceHash suspends operations while it co-operates with authorities over 'professional attack', urging users to change passwords

NiceHash said approximately 4,700 bitcoins were stolen. Photograph: Dado Ruvic/Reuters

Nearly \$64m in bitcoin has been stolen by hackers who broke into Slovenian-based bitcoin mining marketplace NiceHash.



Video 9



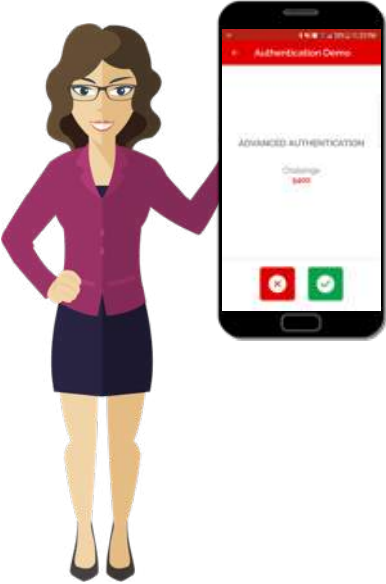
Mimikatz in Real Life (IRL)

- **Mimikatz** is a password/credential stealing tool used by hackers and pen-testers
- Mimikatz remained the #1 malware all 2018

```
.#####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (Apr 26 2014 00:25:11)
.## ^ ##.
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 14 modules * * */
```


Prevention: AuthPoint Secures Log-in

Easy multi-factor authentication (MFA) for:



Employee PC and network login



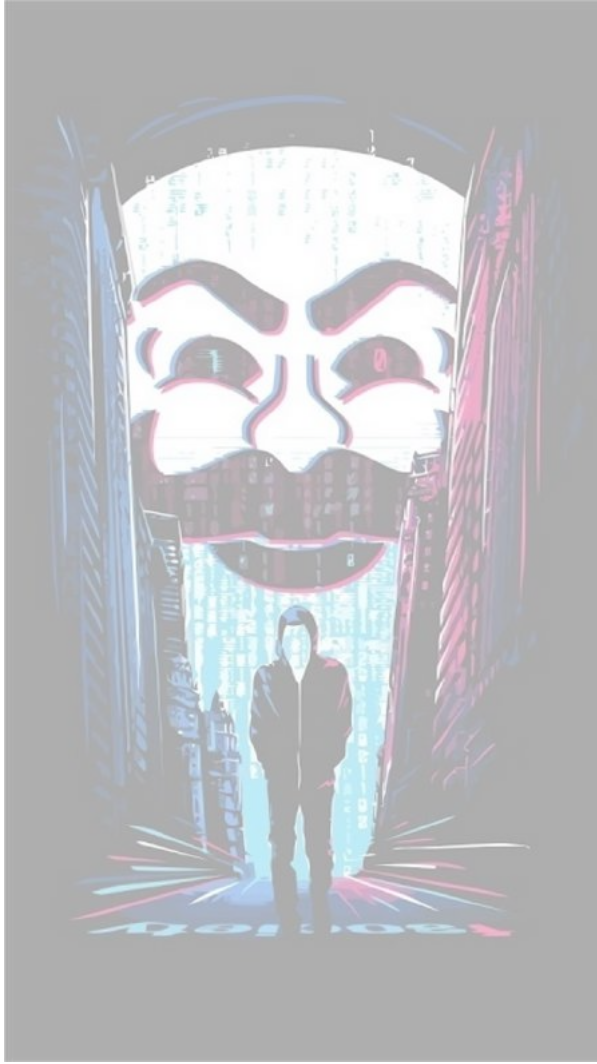
Remote access



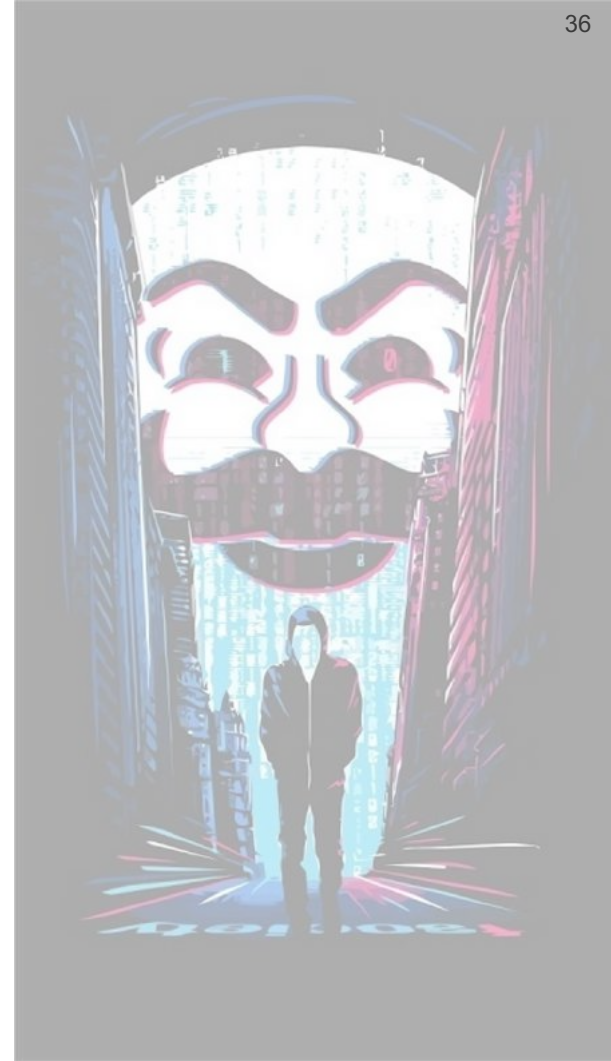
Privileged users access



Access to cloud services (SaaS)



Umfrage 4





19 5322 4587 5437 EXP 03/15 0920 0502.5
ACCESS NO 4884 2943 21620 BALLANCE
41 9876 681 EXP 06/16 4219 9761 6112 A
461 EXP 07/19 ACCT 4568 7701 2494 1344
BALANCE DUE 1214 9487 1101 3487 EXP
17 4200 3771 4045 00 ACCT 8864 3145 34
1245 680 2475 ACCT 4461 7641 9110
110 3497 7704 ACCT 6414 2214 1452 250
528 EXP 07/83 5434 976 BALANCE DUE
41 9876 681 EXP 06/16 4219 976
3 BALANCE DUE 1214 9487 1101 3487 EX
156 29 EXP 07/83 5434 976 BALANCE DUE
RRR PAYE BALANCE 0934 4892 2591 58
4 2943 21620 BALLANCE DUE 08812327
ACCT 4569 7701 2494 1344 OVERDRA
ACCT 4461 7641 9110 3641 33 1640
ACCT 6414 2214 1452 2500 5679.8
85 2365 1478 BALANCE DUE 9084 4245
7 3369 134 EXP 4/18 1936 2387 4561 445
222 4587 5137 EXP 03/15 0920 0502 01
ACCESS NO 4884 2943 21620 BALLANCE
98876 661 EXP 06/16 4219 9761 6112 A
EXP 07/19 ACCT 4569 7701 2494 1344
BALANCE DUE 1214 9487 1101 3487 EXP
15 680 2475 ACCT 4461 7641 9110 3641
200 3771 4045 00 ACCT 8864 3145 3
3487 7704 ACCT 6414 2214 1452 250
29 EXP 07/83 5434 976 BALANCE DUE
ACCESS NO 4884 2943 21620 BALLANCE
3461 EXP 07/19 ACCT 4569 7701 24
1245 680 2475 ACCT 4461 7641 9110
2110 3487 7704 ACCT 6414 2214 1452 2
06/16 01287 41789 2385 1478 BALANCE
3468 235 3696 7368 134 EXP 4/18 1936
CESS 01 1214 ACCESS NO 4884 2943 216
6 6445 0 6552 3461 EXP 07/19 ACCT 456
7/633 20 9754 1245 680 2475 ACCT 446

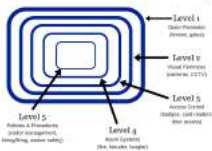
Defense Summary



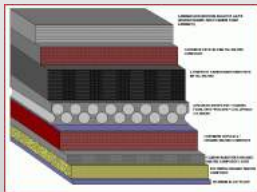
Layered Defense Still Wins...

Secure

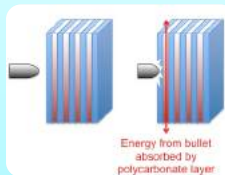
Facilities have five layers of security



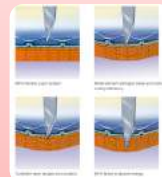
Tank Armor



Bulletproof Glass



Bulletproof Vest



Chemical

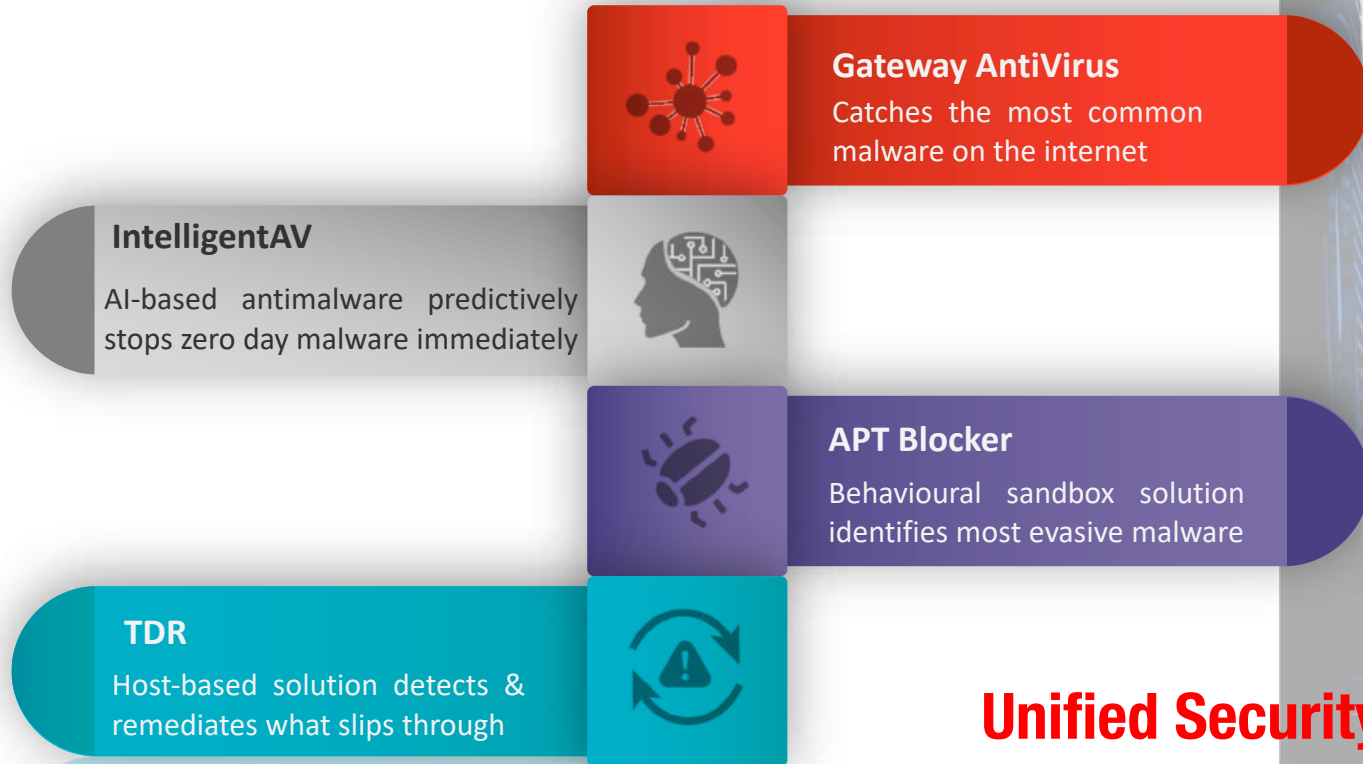


Cyber Security



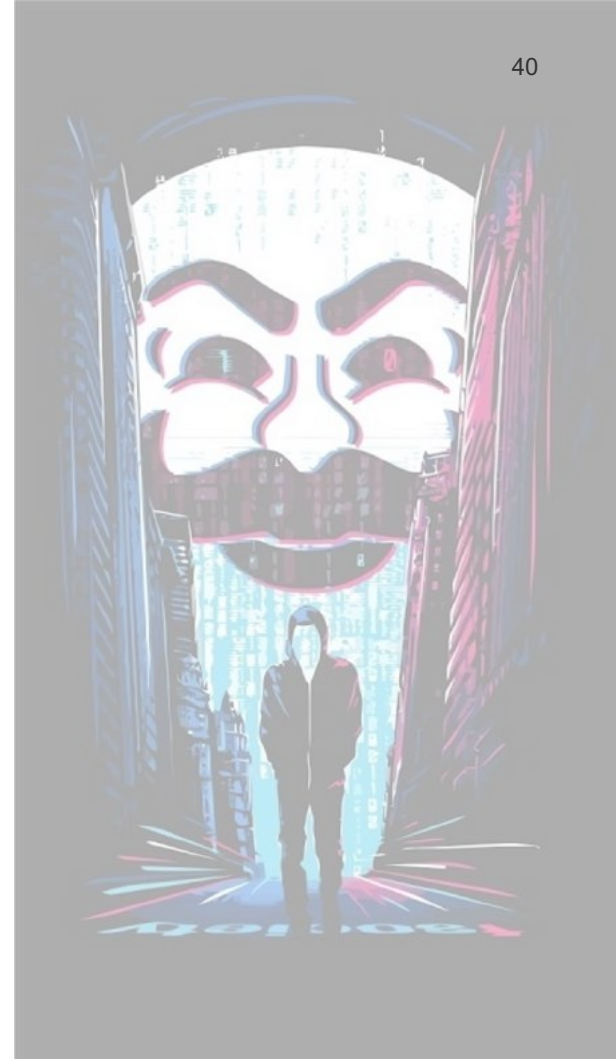
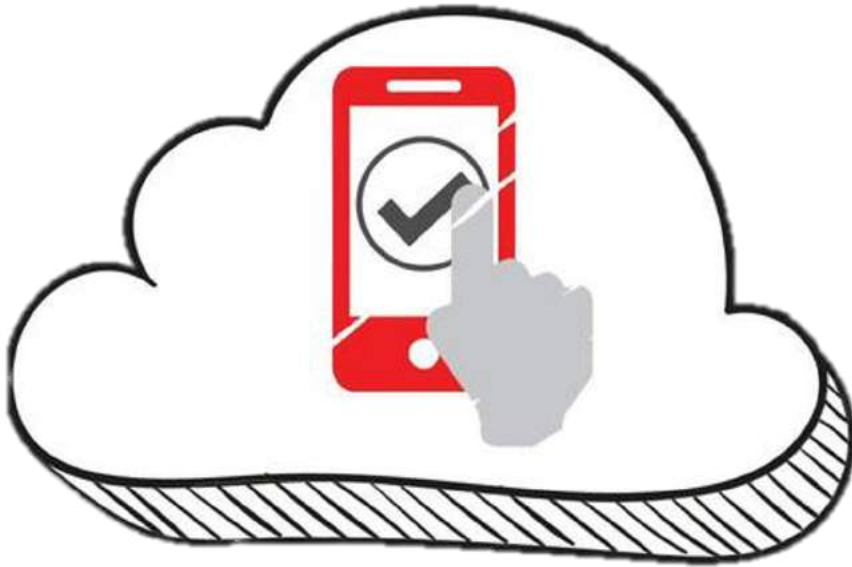
...but here's what to focus on in 2020

2020 Focus: Industry-Leading Advanced Antimalware Pipeline



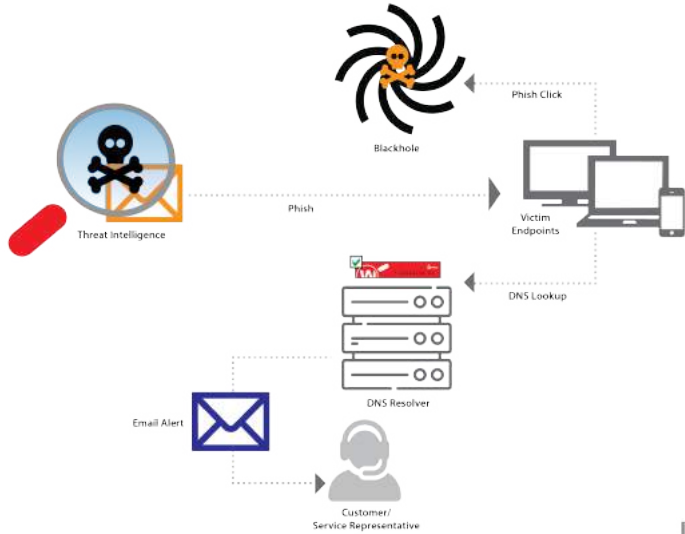
Unified Security Platform

2020 Focus: MFA with AuthPoint



Jetzt für 60 Tage kostenfrei!

2020 Focus: DNS Filtering



DNSWatch

DNSWatchGO

Mr. Robot Rewind: *Analyzing Hackuracy*

Anyway, back to the command. Since I can't find the exact copy of the script, I can only extrapolate what some of the parameters were, but let's break down the command.

- The first parameter of *py* is *"-m artist."* While it's not in the real-world scripts, I'm guessing this parameter puts the script in the mode of searching an artist's library of songs, rather than an individual song.
- The second parameter, *"-i artists.txt,"* defines an input file. Presumably, Elliot created a text file full of musical artists. Since he's trying to crack Romero's passwords, I'm assuming their friendship and familiarity is what allows Elliot to focus on musicians and groups Romero liked. More on why I think that soon.
- The last parameter is *"-o lyrics.txt."* This creates an output file called *txt* that would contain all the results of the lyric searches.

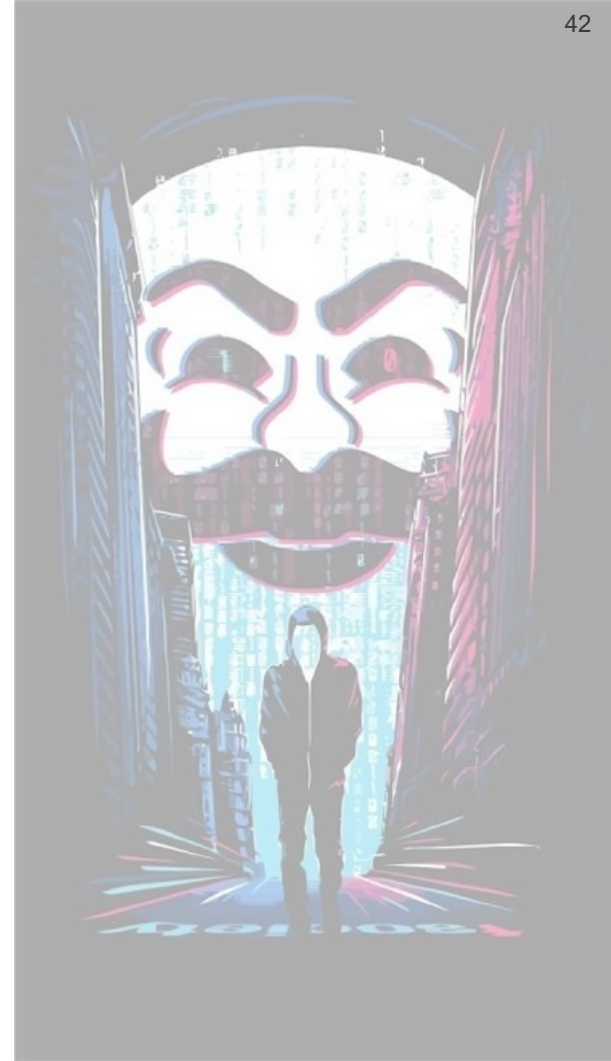
In short, this command would create a text file full of the lyrics from songs and artists that Romero likes. Here's the result of the command, including some of the downloaded artists like Curtis Mayfield.

```
root@kali:~/tools/PyLyrics# python getlyrics.py -m artist -i
Downloading "Curtis Mayfield" (82 songs)
Downloading "Grandmaster Flash and the Furious Five" (20 songs)
Downloading "Isley Brothers" (108 songs)
Downloading "Shamalar" (49 songs)
```

Figure 5: Results of a lyrics search including Romero's favorite musicians.

So why does Elliot need this?

<https://www.geekwire.com/?s=Mr.+Robot+Rewind>



Neuigkeiten

- WatchGuard kündigt Kauf von Panda Security an
- Fast an jedem Tag ein Webinar
- MFA für 60 Tage kostenfrei

Danke

Michael Haas

+49 170 7727415

michael.haas@watchguard.com

