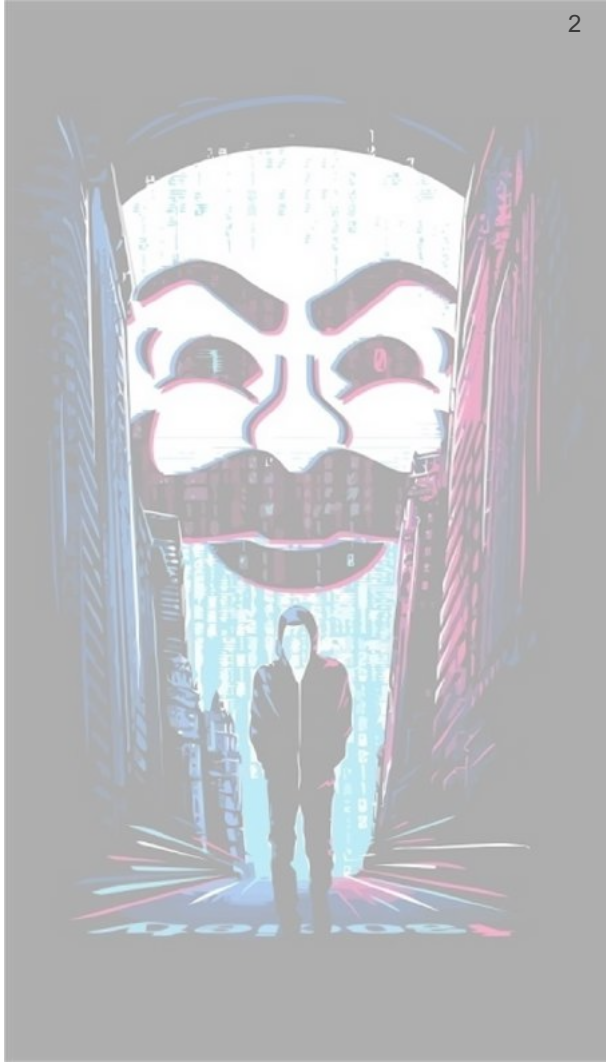
Mr. Reality or Mr. Robot?

Michael Haas – Area Sales Director Central Europe

Umfrage 1



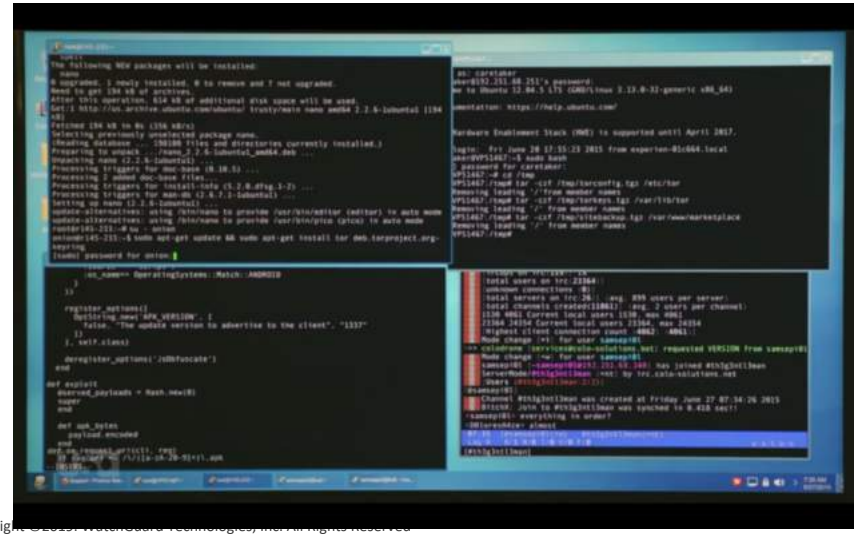
Agenda

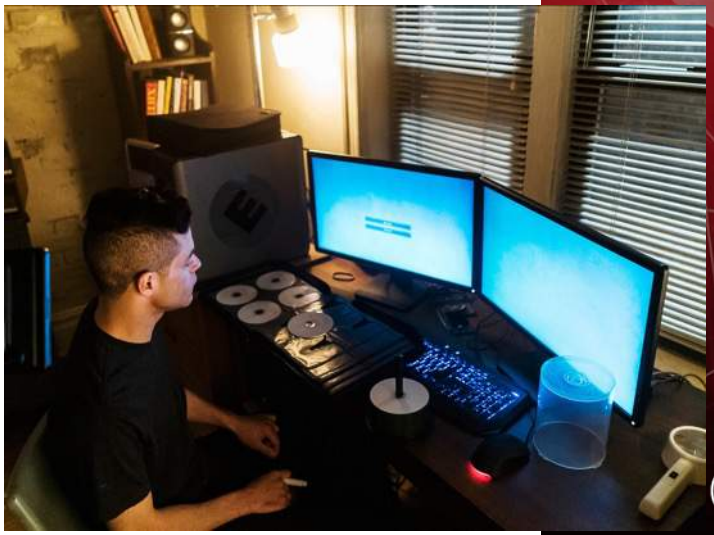
- **Quick Look at Hollywood Hacking**
  - And why Mr. Robot is better
- **Five Real Threats from Mr. Robot**
  - Top threats to beware
  - Mr. Robot examples vs real world
  - Corresponding defenses
- **Summarizing Defense**

Hollywood

Mr. Robot Gets Hacking Right!

- They use the right lingo, the proper way
- They show REAL existing tools
- Only a few missteps, mostly to drive “story”






5 Real-World
Threats
from
MR. ROBOT

Video 1

Video 2 – Theme #1

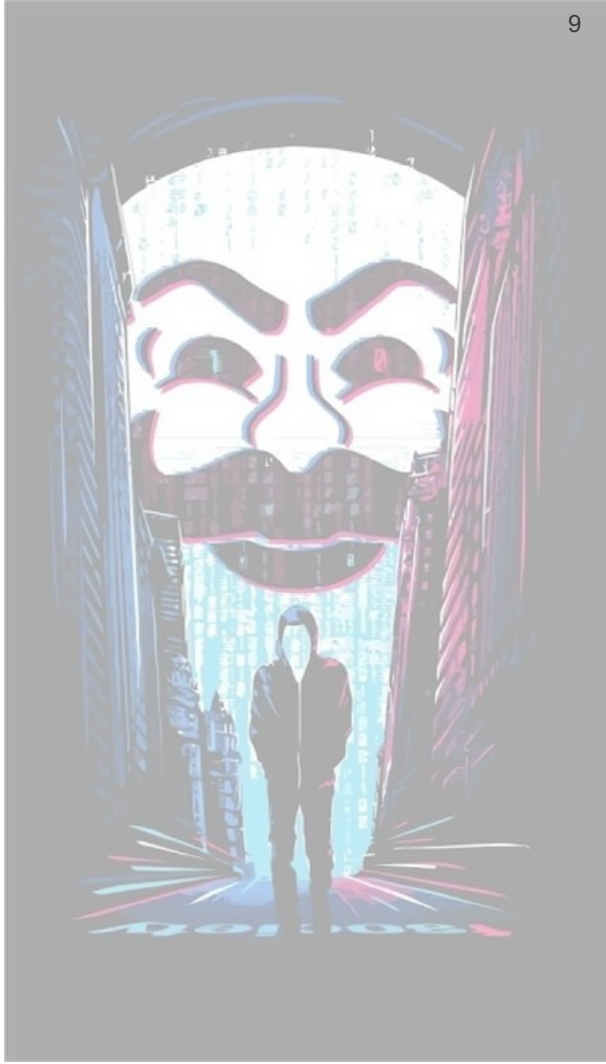
Theme #1: **Phishing**

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

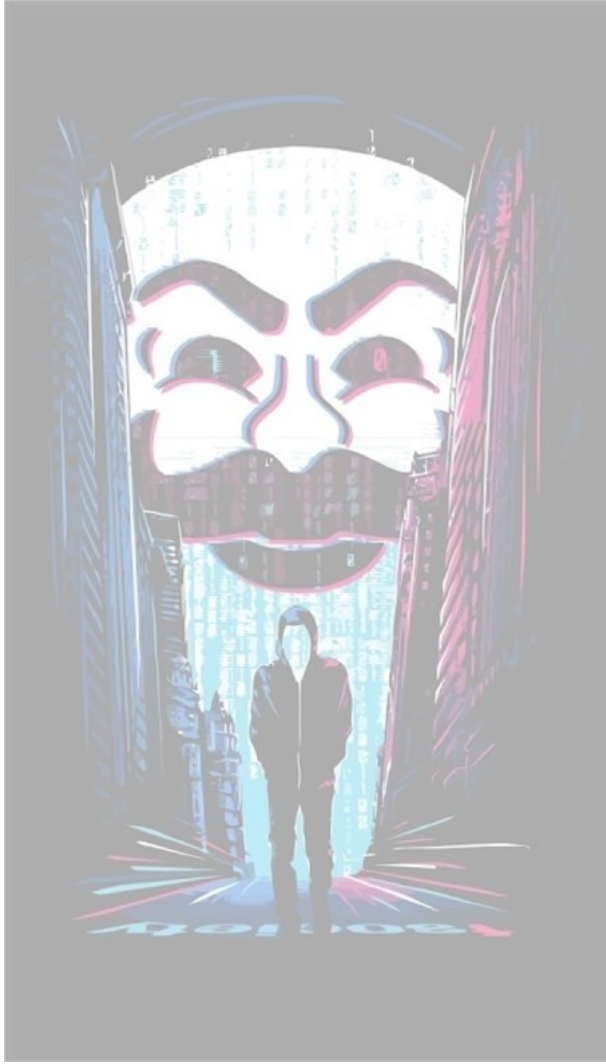
Phishing – luring a victim into giving up credentials or doing something via a legitimate seeming email

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

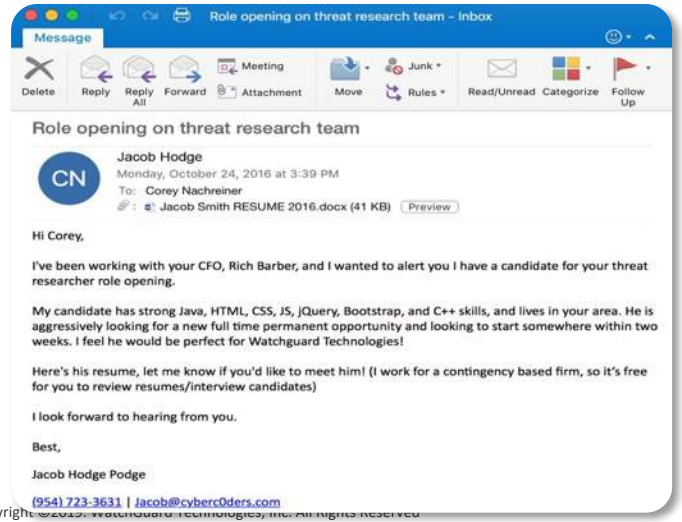


Flavors of Phishing

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

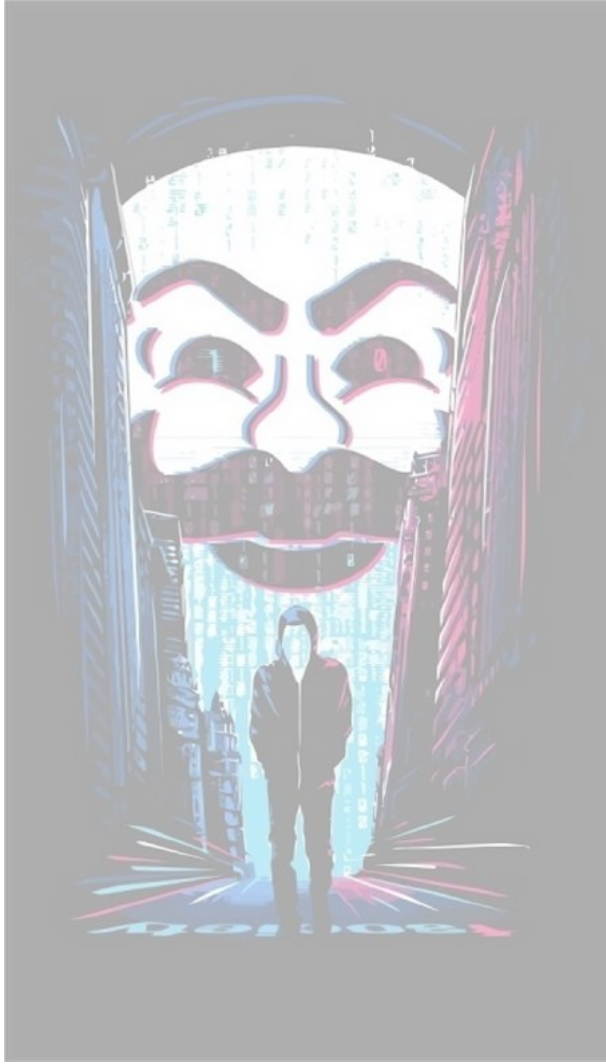
Spear-phishing – A more customized phishing email that targets a specific individual or group

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

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 loc

Cheers,

John Smith

john.smith@CNN.com

nd yet they click

50%

0%

Study 1: a

clicke

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

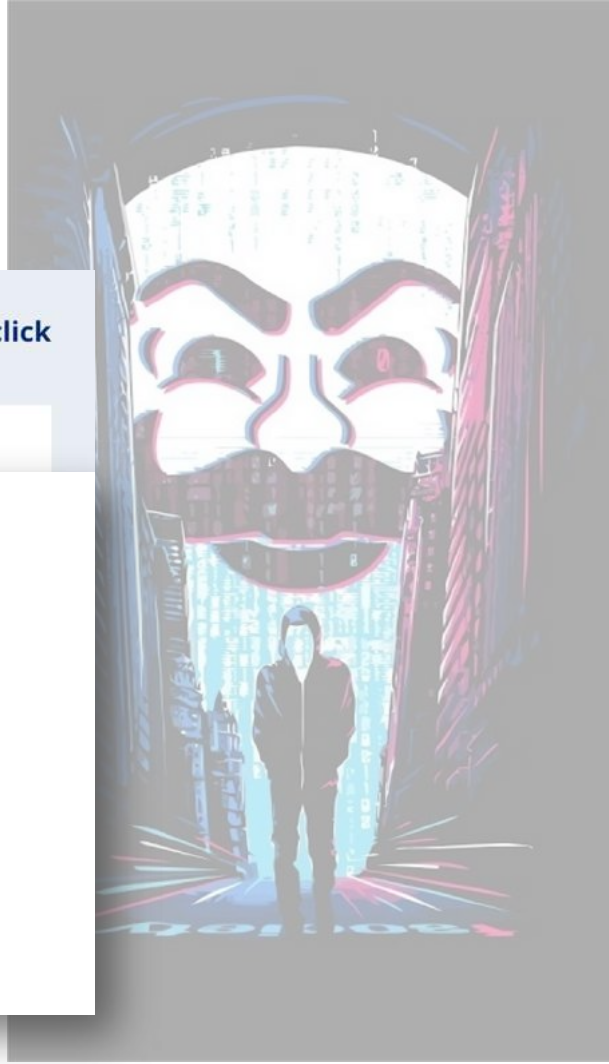
If you do not wish to review this paper, please click this link:

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

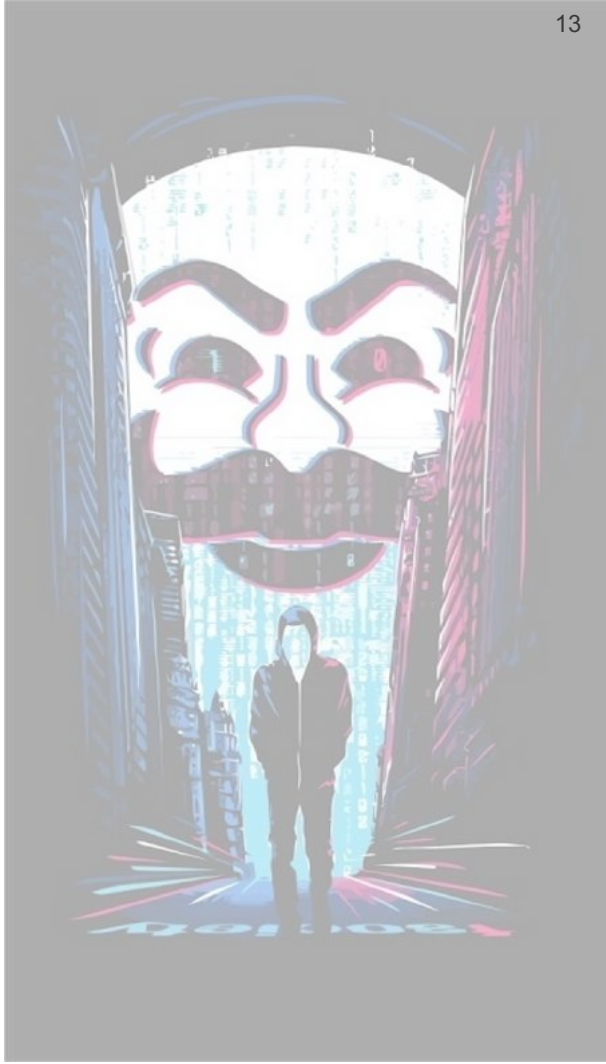
Best regards,

Editor

<name I've never heard of>



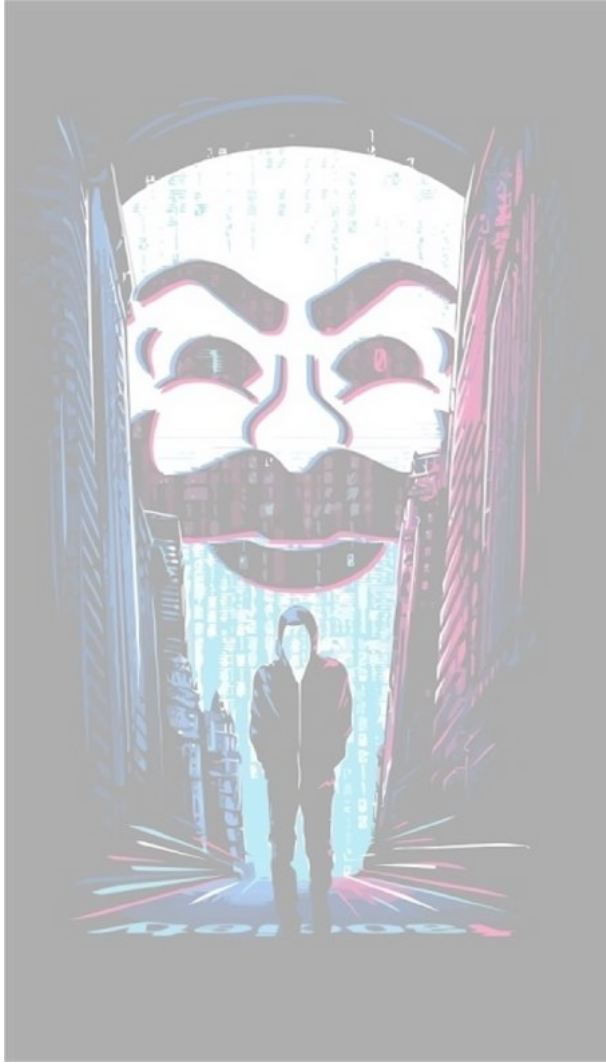
Umfrage 2



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 Ransom*WORM*

Mr. Robot

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

Ransomware Hitting State and Local

Baltimore city government computer network hit by ransomware attack

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

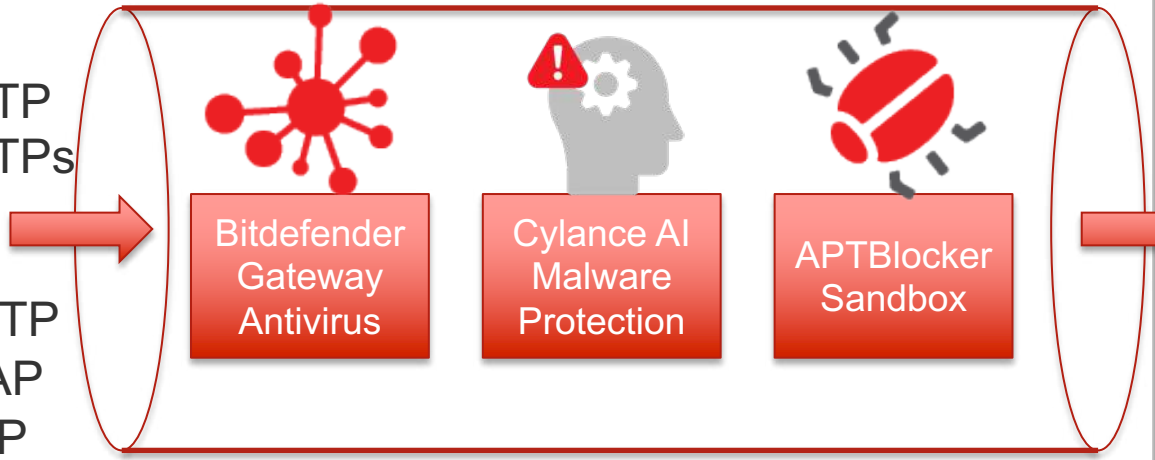
The state declined to say which towns were affected by the coordinated cyberattack. But one expert said it could signal more such attacks in the future.

Prevention: Advanced Malware Detection

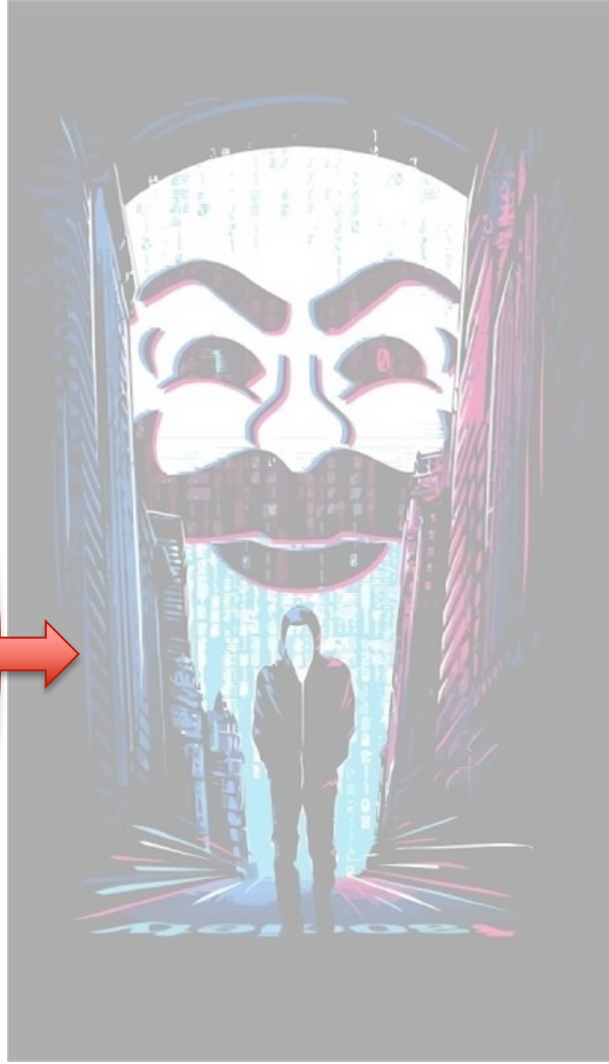
The most advanced malware protection on the market

Web
- HTTP
- HTTPs

Email
- SMTP
- IMAP
- POP



Others…



Video 4 – Theme #3

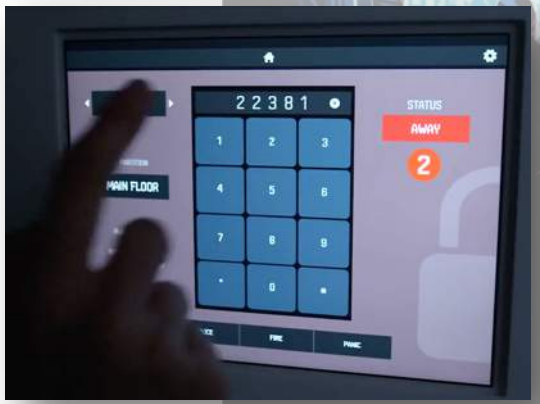
Theme #3: **IoT Attacks**

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

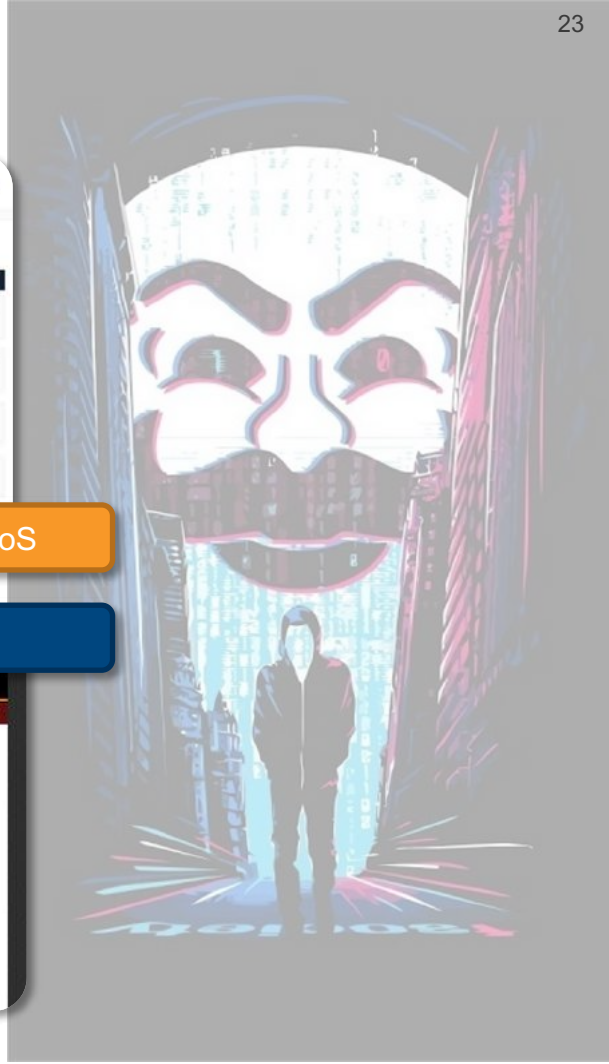
IoT Attacks Build Off Mirai

Krebs hit with 620Gbps DDoS

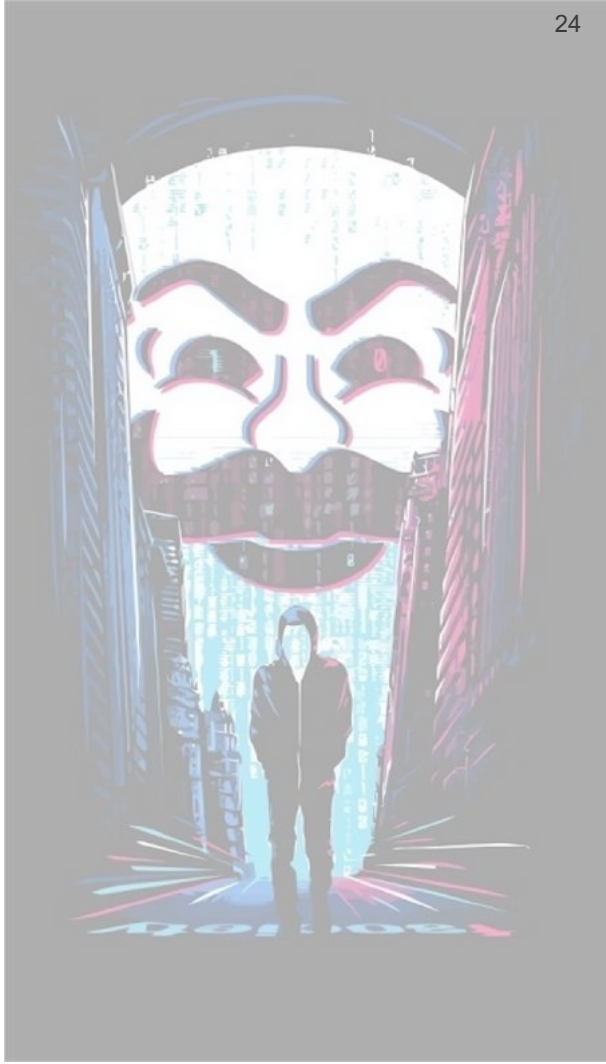
OVH hit with 1Tbps DDoS

IoT DDoS targets DNS

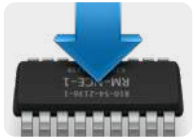
Mirai Copycats

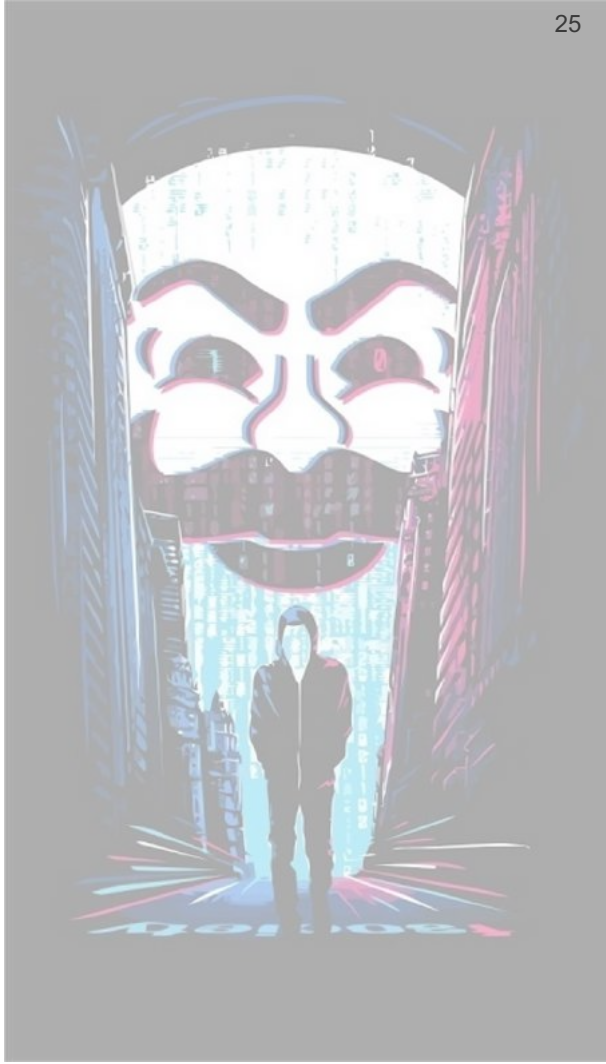


Umfrage 3



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

Secplicity®
Security Simplified

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

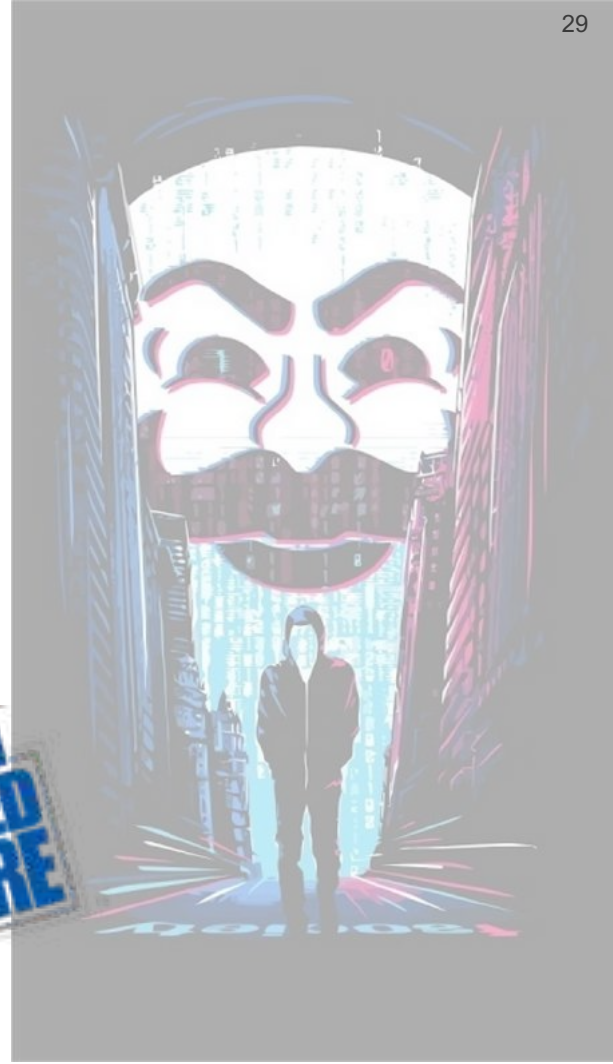
	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Test	**Detect**	**Prevent**	**Detect**	**Prevent**	**Detect**	**Prevent**	**Detect**	**Prevent**
Rogue AP	P	P	F	*N/A*	F	MP	F	*N/A*
Rogue Client	P	P	F	*N/A*	F	MP	*N/A*	MP
Neighbor AP	P	P	P	P	F	*N/A*	F	*N/A*
Ad-Hoc Network	P	P	F	*N/A*	F	*N/A*	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 Mohit Kumar

Tweet Share Share

PAS

****

1.4 Bi

Hackers always first go for the weakes

13 MAR 2017 NEWS

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

Tara Seals US/North Am

Email Tara

In the latest settlemen Depot, the retailer has

Illustrating the real-wo breach is ultimately goi much more once legal f

The 2014 incident, whic credit-card compromise that file valid claims wil losses, even if they have their losses may get an

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 undergrou to steal customer's passwords.

JOSEPH COX 11.23.17 8:41 AM ET

Where there's a data breach, there they don't have access to the ream

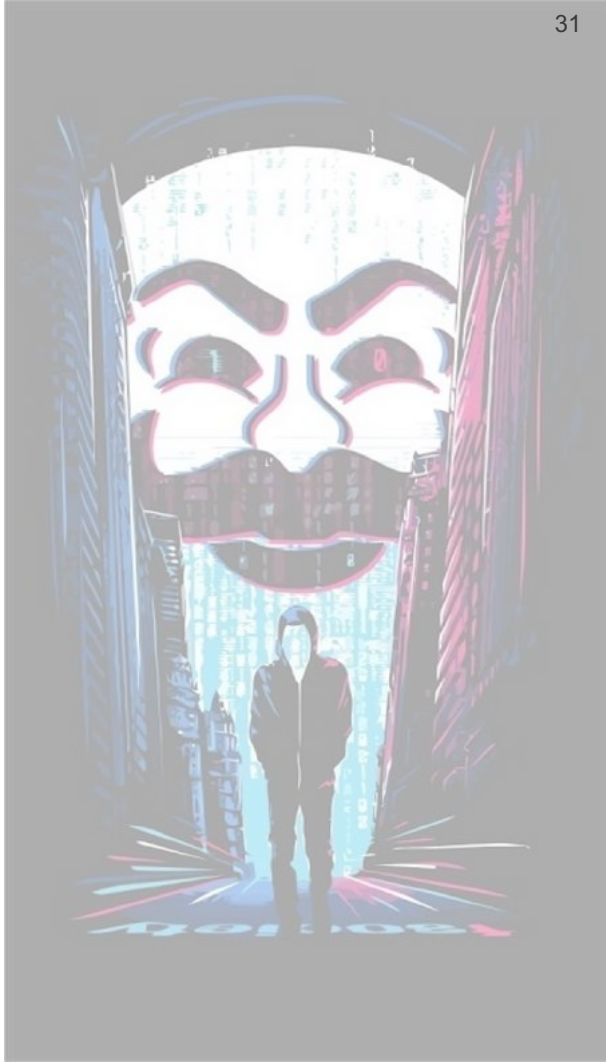
On Tuesday Bloomberg reported t 2016 breach of 57 million account phone numbers of 50 million ride news by sending potential Uber us steal their password.

Bitcoin: $64m in cryptocurrency stolen n 'sophisticated' hack, exchange says

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

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

early $64m in bitcoin has been stolen by hackers who broke into Slovenian-ased bitcoin mining marketplace NiceHash.

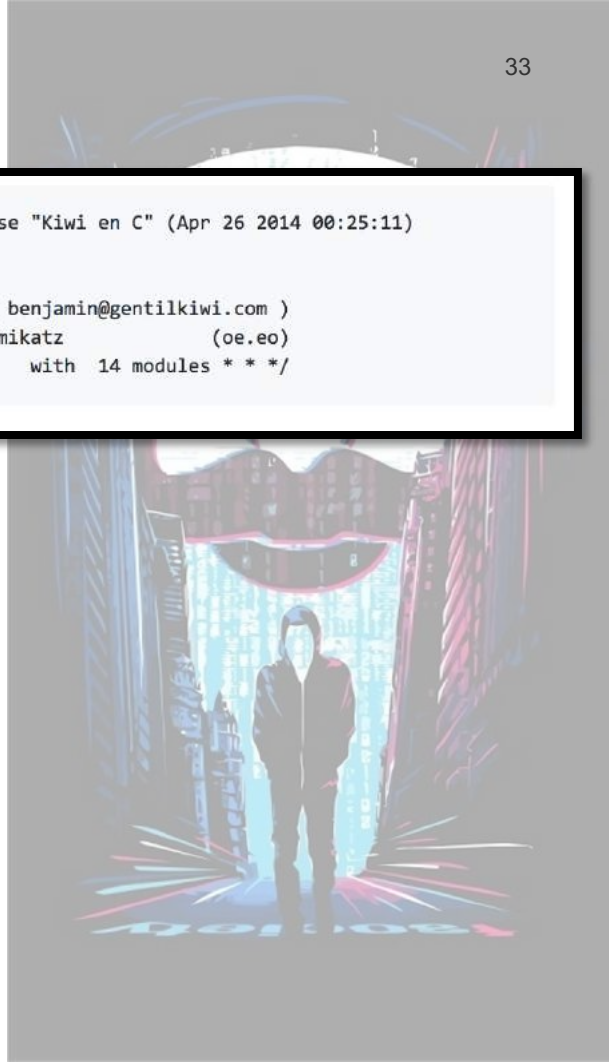


Video 9

Mimikatz in Real Life (IRL)

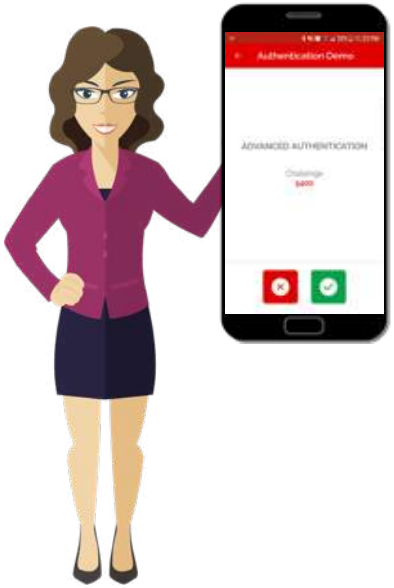
- ***Mimikatz*** is a password/credential stealing tool used by hackers and pen-testers
- Mimikatz remained the #1 malware all 2018

```
  .#####.   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:

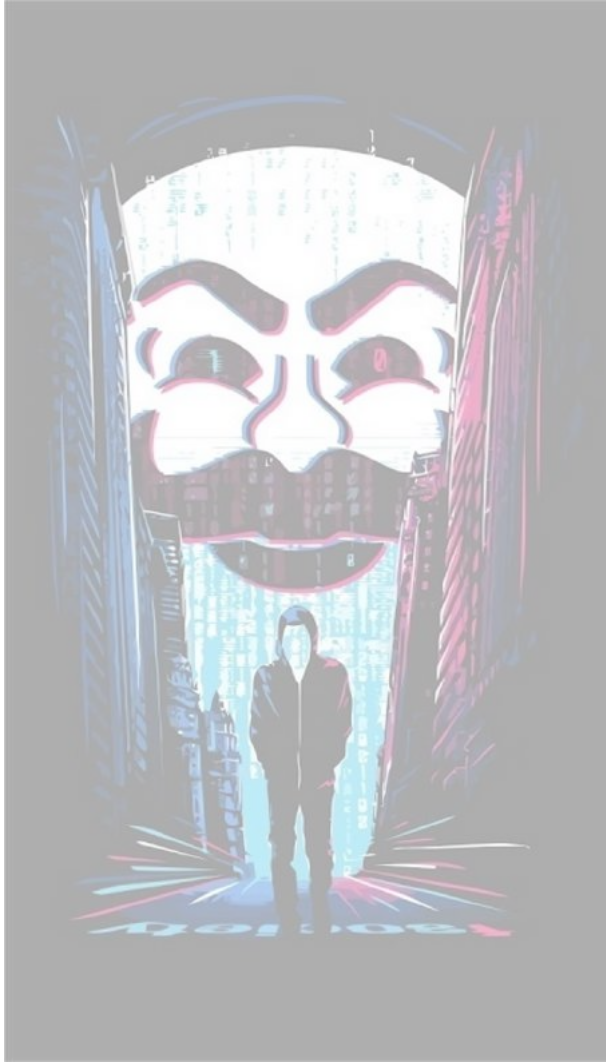


Employee PC and network login

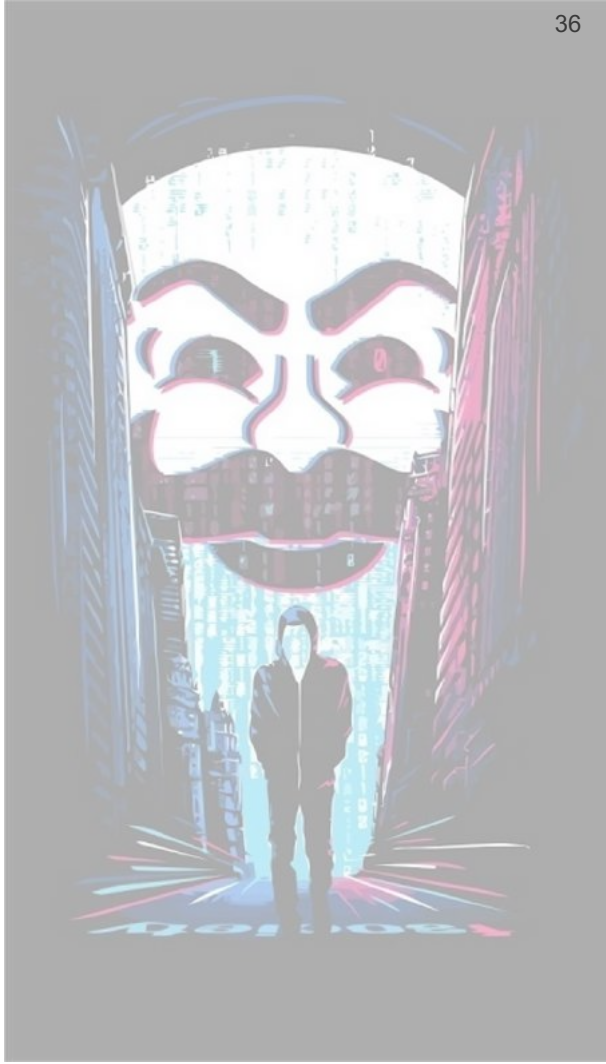
Remote access

Privileged users access

Access to cloud services (SaaS)



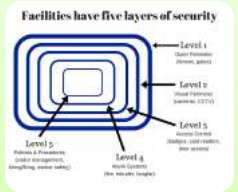
Umfrage 4



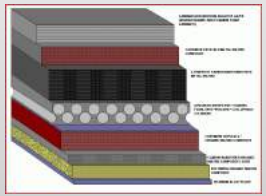

WatchGuard
Defense Summary

Layered Defense Still Wins…

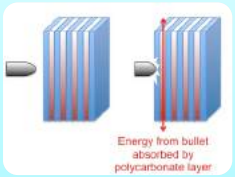
Secure



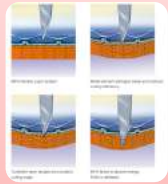
Tank Armor



Bulletproof Glass



Bulletproof Vest



Chemical

Cyber Security

…but here's what to focus on in 2020

2020 Focus: Industry-Leading Advanced Antimalware Pipeline

Gateway AntiVirus
Catches the most common malware on the internet

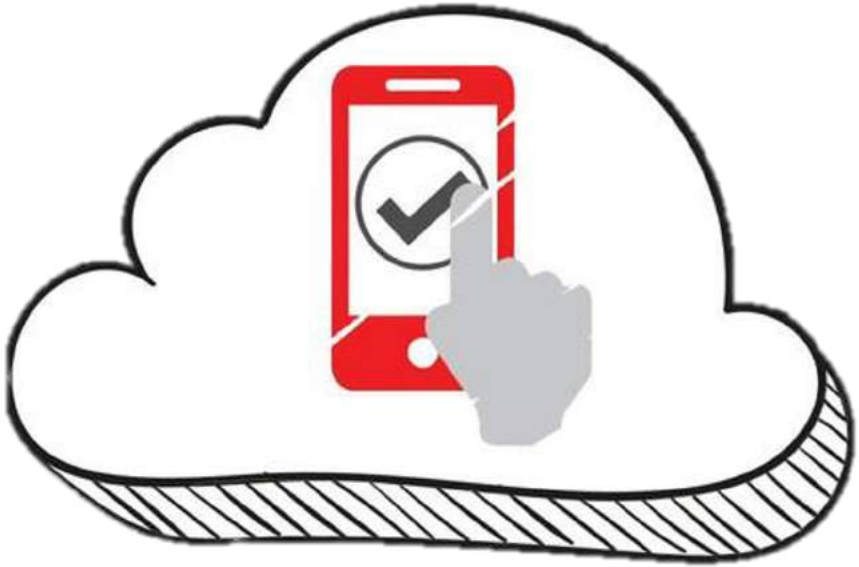
IntelligentAV
AI-based antimalware predictively stops zero day malware immediately

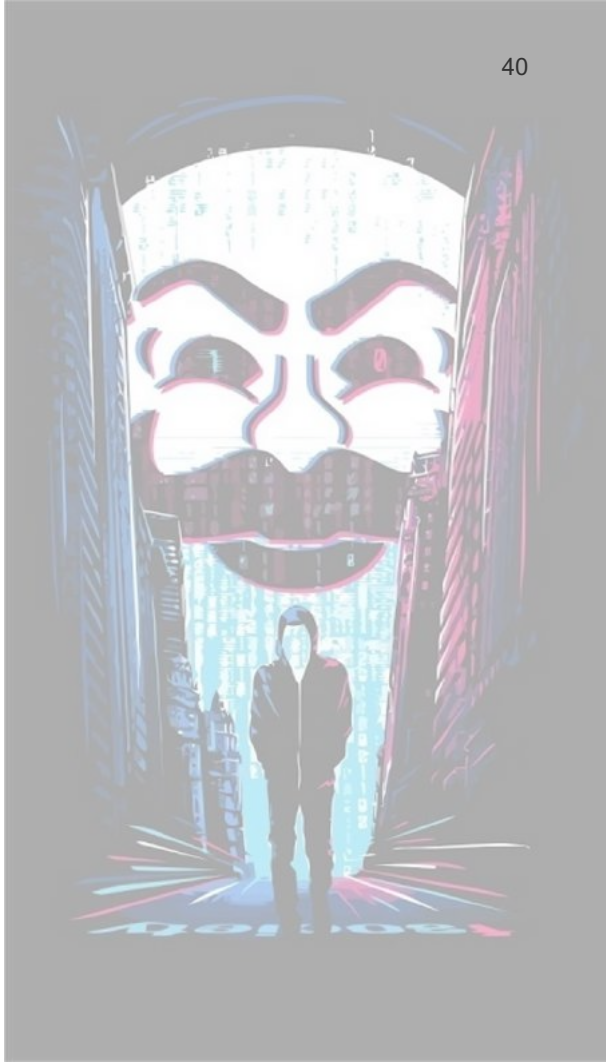
APT Blocker
Behavioural sandbox solution identifies most evasive malware

TDR
Host-based solution detects & remediates what slips through

Unified Security Platform

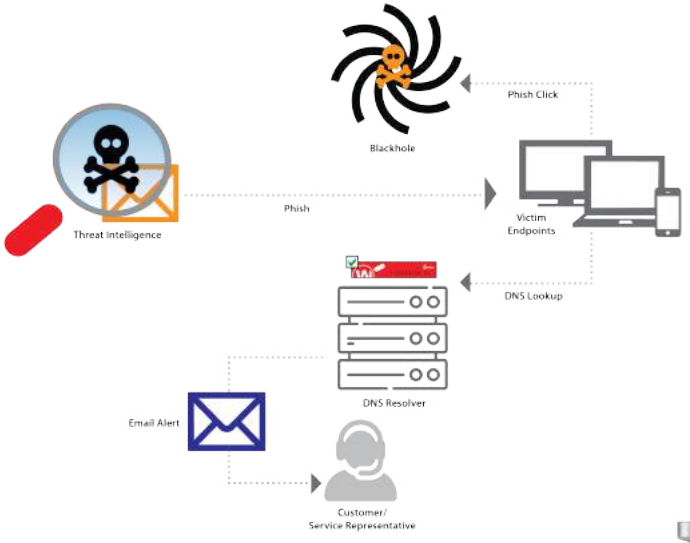
2020 Focus: MFA with AuthPoint





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.

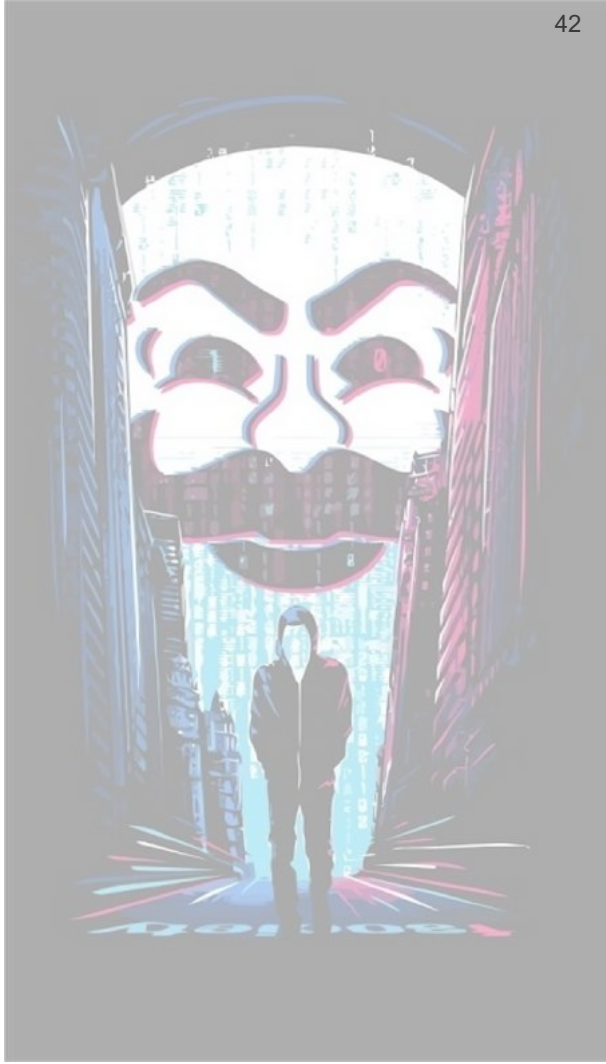
- The first parameter of *py* is "*-m artist*." While it's not in the real-world scripts, I'm guessing this parameter puts the script in the mode of searching an artist's library of songs, rather than an individual song.
- The second parameter, "*-i artists.txt*," defines an input file. Presumably, Elliot 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 song
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