EdgeCon
ANNUAL CONFERENCE 2020

Patrick Pocalyko
EVP, US Operations

Cyber Security vs. Cyber Defense

Perception vs. Reality…

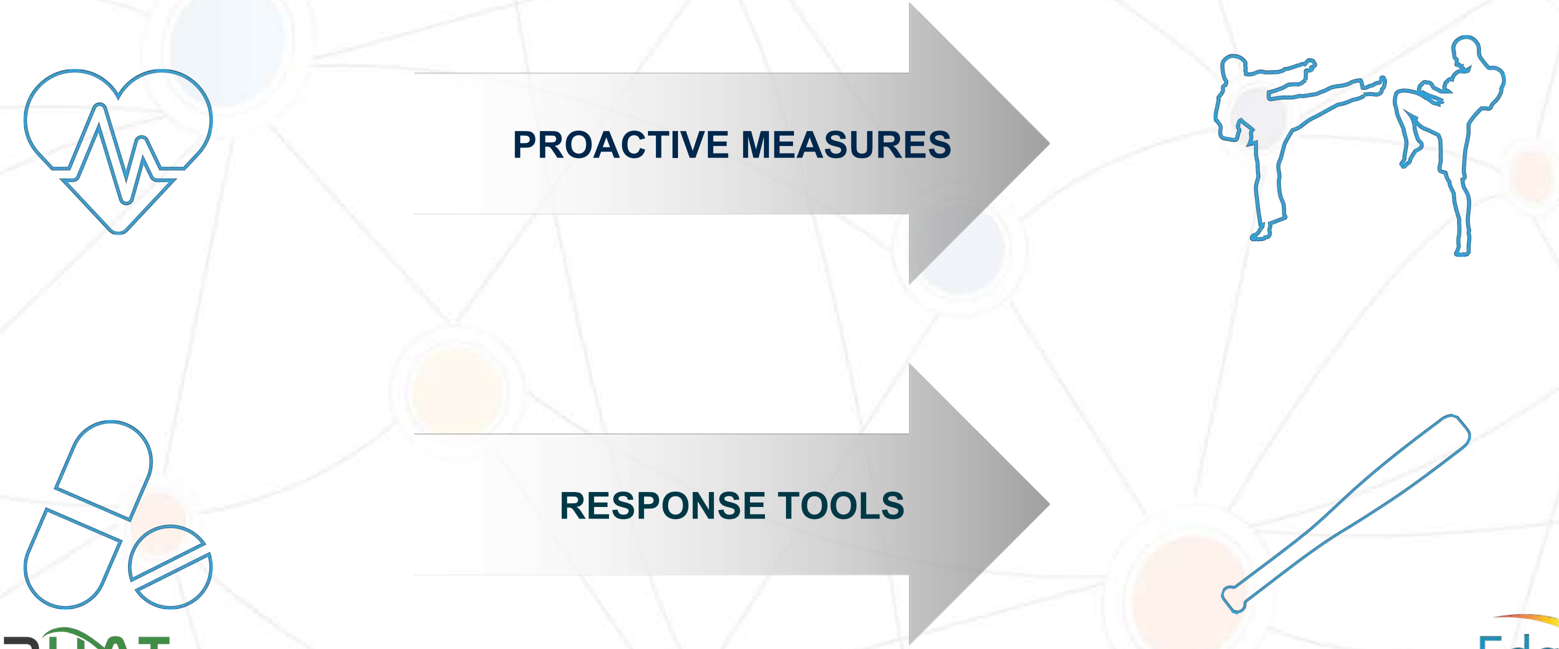
CYBERHAT
proactive cyber defense

CYBER SECURITY (HEALTH) VS CYBER DEFENSE (PROACTIVE MEASURES)

THE PHYSICAL WORLD

HEALTH

PROACTIVE MEASURES



PROACTIVE MEASURES

RESPONSE TOOLS

CYBER SECURITY (HEALTH) VS CYBER DEFENSE (PROACTIVE MEASURES)

OUT SOURCING

HEALTH

Service Organization Controls 1 (SOC 1), Type II report.
Service Organization Controls 2 (SOC 2), Type II report.
Service Organization Controls 3 (SOC 3) report.

PROACTIVE MEASURES

Hacking Simulations

Proactive Intelligence

Offensive Minded Assessments

THE REALITY

So… what does it take to bypass a $ 105M security budget?

* Best of bread Antivirus software

* EDR – (Endpoint Detection Response) Endpoint protection advanced systems

* Cisco AMP – malware protection- intelligence system

* IPS / IDS- Intrusion Prevention and Detection System

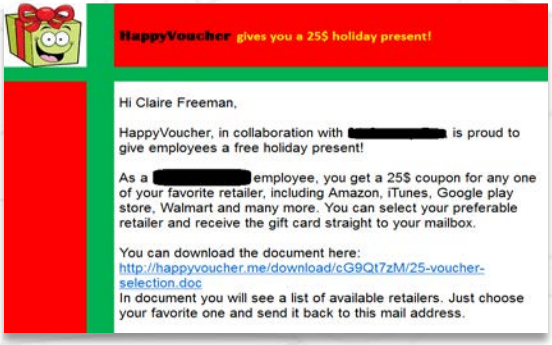
* Firewalls, network, DB and WAF

* Anomaly detection advanced analytics security system

* SIEM , IR team….. And on and on an on…..

THE EXECUTION

Phishing



HappyVoucher gives you a 25$ holiday present!

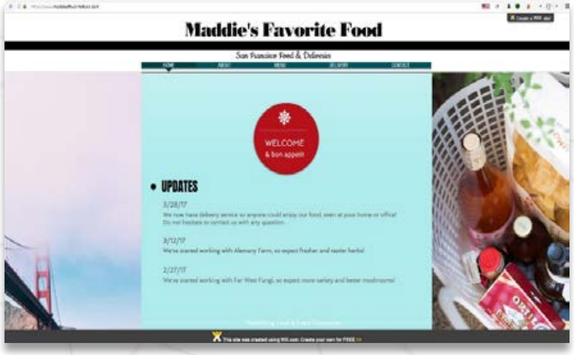
Hi Claire Freeman,

HappyVoucher, in collaboration with [redacted] is proud to give employees a free holiday present!

As a [redacted] employee, you get a 25$ coupon for any one of your favorite retailer, including Amazon, iTunes, Google play store, Walmart and many more. You can select your preferable retailer and receive the gift card straight to your mailbox.

You can download the document here:
http://happyvoucher.me/download/cG9Qt7zM/25-voucher-selection.doc
In document you will see a list of available retailers. Just choose your favorite one and send it back to this mail address.

Social Engineering



Maddie's Favorite Food

San Francisco Food & Deliveries

- UPDATES

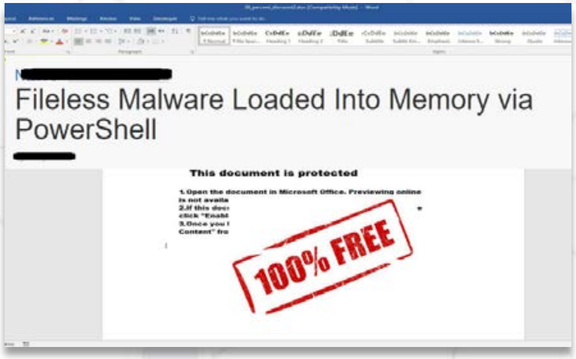
3/28/17
We now have delivery service so anyone could enjoy our food, even at your home or office! Do not hesitate to contact us with any question.

3/12/17
We've started working with Alemany Farm, so expect fresher and tastier herbs!

2/27/17
We've started working with Far West Fungi, so expect more variety and better mushrooms!

This site was created using WIX.com. Create your own for FREE >>

The Payload



[redacted]

Fileless Malware Loaded Into Memory via PowerShell

[redacted]

This document is protected

1. Open the document in Microsoft Office. Previewing online is not availa
2. If this doc
click "Enabl
3. Once you
Content" fro

The COST

FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
FF 95594731 A
F 6
100
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
ONE HUNDRED DOLLARS
FRANKLIN

THE EXECUTION

3 DAYS OF ROAMING AROUND THE NETWORK

- Internal Port Scanning
- Internal vulnerability scans
- Network "hopping"
- Data recon (67 user names & Passwords acquired)
- 26 Machines "Admin take over"

POSITIONING ESTABLISHED

SECURITY IN PLACE

SOPHOS

TWO-FACTOR AUTHENTICATION PROTECTS YOUR ACCOUNT IN THE EVENT THAT YOUR PASSWORD IS STOLEN.

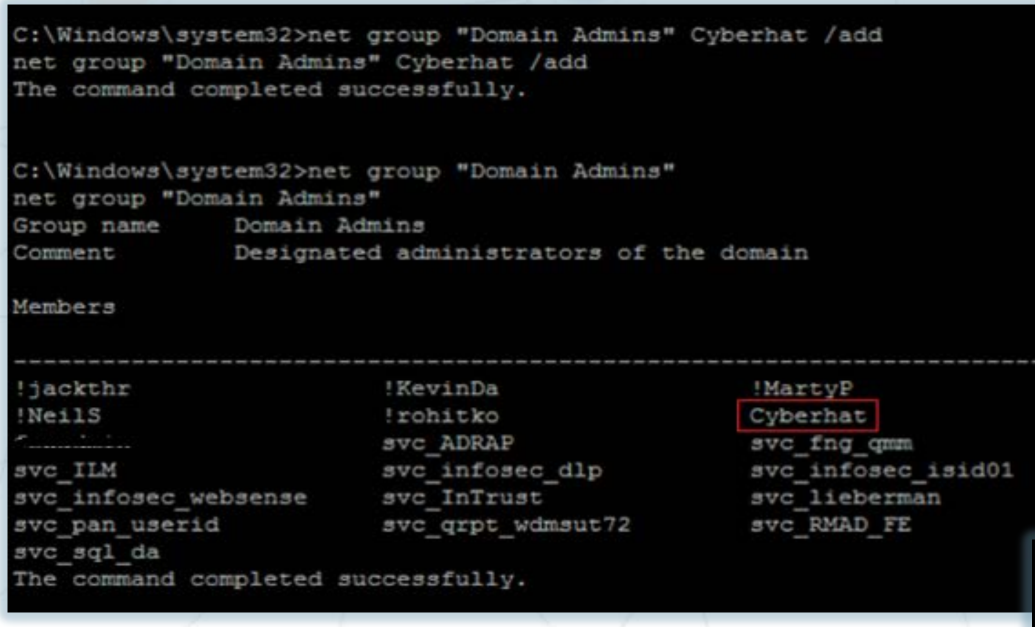
ChangeAuditor

Quest® ChangeAuditor®

Profile: MS9.domain9.local - DEFAULT

□ Auto Connect

THE EXECUTION



```
C:\Windows\system32>net group "Domain Admins" Cyberhat /add
net group "Domain Admins" Cyberhat /add
The command completed successfully.


C:\Windows\system32>net group "Domain Admins"
net group "Domain Admins"
Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
!jackthr                 !KevinDa                 !MartyP
!NeilS                   !rohitko                 Cyberhat
[redacted]               svc_ADRAP                svc_fng_qmm
svc_ILM                  svc_infosec_dlp          svc_infosec_isid01
svc_infosec_websense     svc_InTrust              svc_lieberman
svc_pan_userid           svc_qrpt_wdmsut72        svc_RMAD_FE
svc_sql_da
The command completed successfully.
```

In Closing

CYBER SECURITY vs CYBER DEFENSE

Thank you!