Lend me your IR's!

Matt Scheurer
@c3rkah
PDF http://slides.dfirmatt.com

Slide deck initializing...

D3F C0N

BLUE TEAM VILLAGE

IR

```
if (badEvent == "true") {
   perform = "Incident Response";
}
```

IR

What I do...

I work for a big well-known organization...

As an Assistant Vice President (AVP) of Computer Security and Incident Response (IR). However, I have many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).

I am also a Podcast Host for

ThreatReel

https://threatreel.com

Where I volunteer...

I am an Official

HACKING IS NOT A CRIME

Advocate

https://www.hackingisnotacrime.org/

I am also a

WOMSA

Empowering Women in Cybersecurity

Women’s Security Alliance (WomSA) Technical Mentor

https://www.womsa.org/

Disclaimer!

Yes, I have a day job.
However…

Opinions expressed are based solely on my own independent security research and do not express or reflect the views or opinions of my employer.

Objectives

- Show live-demo reenactments of real attacks
  - How these real world attacks worked
  - How & why they defeated security solutions
- Show Incident Responses to these attacks
  - Demo investigation tools and techniques
  - Discuss lessons learned and takeaways

Acronyms Used

- IOC (or “IoC”)
  - Indicator Of Compromise
- IR
  - Incident Response
- DFIR
  - Digital Forensics & Incident Response

Other Disclaimers

- Demos are all based on 100% true stories
  - These demos dutifully recreate actual attacks
  - However, some details were altered
- Investigation demos are sped up considerably
  - In the interest of allotted presentation time
- Only perform these techniques in a dedicated securely isolated and volatile sandbox!

Scenario #1

“The Mystery Attachment”

Preface

News Headline from August 17, 2018:
“*Malspam Campaign Targets Banks Using Microsoft Publisher*”

The “FlawwedAmmy RAT” was part of the “Necurs botnet” as reported by researchers at Trustwave.

Reference: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/malspam-campaign-targets-banks-using-microsoft-publisher/

The following week...

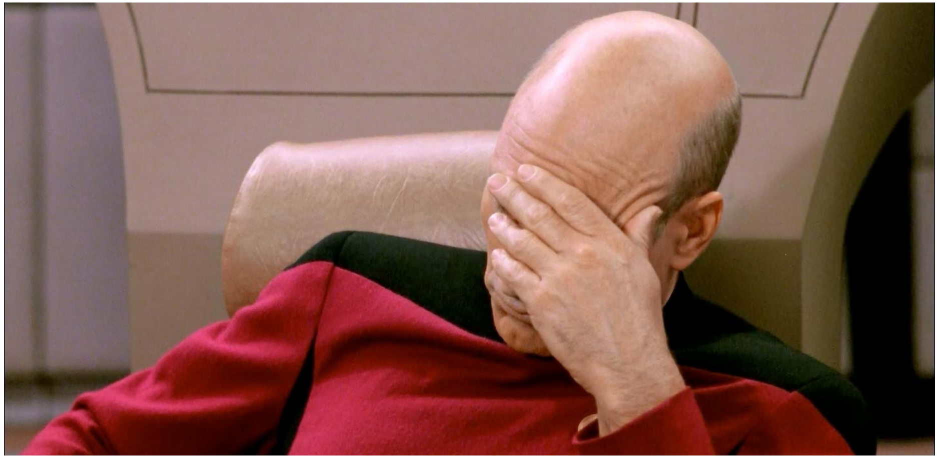
Matt! Help!! One of our VIP's with access to lots of very sensitive information just got hit in that recent malspam campaign targeting banks. It matches the IOC's from reports of that new FlawedAmmyy RAT which is part of the Necurs botnet! The recipient attempted to open the MS Publisher attachment on their smart phone. I need you to drop whatever you are doing and investigate this. We'll get you the attachment ASAP!!!

Investigation

- Open the file (Demo) in a Sandbox
  - Detonation, research, attempts and failure to understand anything about this “malicious file”
    - Strings (Demo)
    - Hash (Demo) & Search
    - Check EXIF data (Demo), while pondering my next steps...

DERP!!!

That Facepalm Moment...



When you realize that the email attachment you’ve just spent the past 3+ hours analyzing actually came from your test phishing vendor!

Validation

I checked the email message headers, and they were what I expected, but I read it like this...

Received: from mail-server.your.test-phishing.company (mail-server.your.test-phishing.company. [**Yes Matt, this really is your test phishing vendor’s IP address, YOU DOLT!**])

What went wrong?

- I got caught up in the moment by subconsciously letting somebody else influence my investigation
- Their anxiety and assumptions wore off on me
- Always start with the message headers when investigating phishing emails and contents!
  - I abandoned my own standards this one time by focusing on the file attachment first

Remediation

- The road to redemption
  - Painful lessons learned for reminders to stick to my standard investigative processes and procedures
  - Had I started my investigation by inspecting the message headers first I could have closed out the investigation in minutes instead of hours
- No further technical actions required

Scenario #2

“Security Scanner Evasion”

Preface

- Identical phishing email starts hitting Inboxes
  - Wide-scale reports of phishing come pouring in
- The phishing page link no longer appears to be working in my security scanner.
  - Was this malicious site taken offline already?
    - Let’s investigate and find out...

Investigation

- Check the email message source code (Demo)
  - Note hyperlinks
- Checking the landing page with a security scanner (Simulation Demo)
- Checking the landing page source code (Demo)
- Open the phishing page (Demo) in a Sandbox

Results

- How the evasion code works
  - Browser User-Agent string based redirection
- Thoughts
  - Source could be hidden with server-side languages (ASP.NET, CGI, Java, Perl, PHP, Python, Ruby, etc.)
  - Could target specific browsers or browser versions using exploit kit round-robin redirects

Remediation

1) Determined the actual phishing landing page and blocked through web content filtering.

2) Worked with our secure email gateway vendor to block the active phishing campaign.

Scenario #3

“The Rabbit Hole”

Preface

- I received a request from a user to investigate an email message they received to determine if it is legitimate or not

- The email appears “Phishy” at first glance, but “*Is it just suspicious or is it malicious?*”

The Investigation

- I can tell from the message headers that the source IP address is a mismatch for the senders domain
- The message source code is particularly interesting...
  - Link text does not match the hyperlink destination (Demo)
- The malicious threat actor’s objective appears to be a credential harvesting site (Demo) for the purposes of Account Take Over (ATO)

Destination #1

- The landing page appears to go to a compromised web host in a foreign country, but does it stop there?
- Obtain the page source to find out (Demo)

Destination #2

- The next landing page appears to go to a compromised web host in a different foreign country, but does it stop there?
- Obtain the page source to find out (Demo)

Destination #3

- That landing page appears to go to a compromised web host in yet another foreign country, but does it stop there?
- Obtain the page source to find out (Demo)

Encoded Content

- The malicious threat actor has used JavaScript encoding to avoid analysis and detection, while hiding the page source (Demo)
  - Decoding the page source using the built-in browser developer tools (Demo)

Encoded Elements

- Whether the threat actor used encoded elements to avoid analysis and detection, or keep the entire site as a single page file, they used Base64 encoded elements (Demo) within their JavaScript encoded page.
  - Decoding the Base64 page elements using the built-in browser developer tools (Demo)
  - And decoding page elements by hand (Demo)

Remediation

1) Determined the final phishing landing page and blocked through web content filtering.

2) Blocked intermediary compromised web servers through web content filtering.

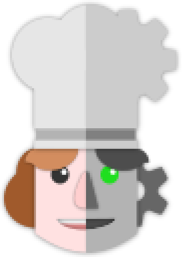
3) Reported compromised web sites to domain owners and hosting companies through their WHOIS contact records

Epilogue

In the time since these original investigations, I’ve learned **CyberChef**. I’ve used **CyberChef** often for file analysis in recent years.

CyberChef:

The Cyber Swiss Army Knife



https://gchq.github.io/CyberChef/

Please check out my free “CyberChef Workshop”...
https://www.ohioinfosec.org/files/2021/CyberChef_Workshop.zip

In Closing

As you see me hanging out on Discord or at DEF CON, please share your own DFIR stories...

In Closing

As you see me hanging out on Discord or at DEF CON, please share your own DFIR stories...

Friends, Romans, DEF CON Attendees,

In Closing

As you see me hanging out on Discord or at DEF CON, please share your own DFIR stories...

Friends, Romans, DEF CON Attendees,
“**Lend me your IR’s!**”

Questions

Who?

What?

When?

Where?

Why?

How?

Lend me your IR's!

Matt Scheurer
@c3rkah
PDF http://slides.dfirmatt.com

Thank you for attending!

```
if (badEvent == "true") {
  perform = "Incident Response";
}
```