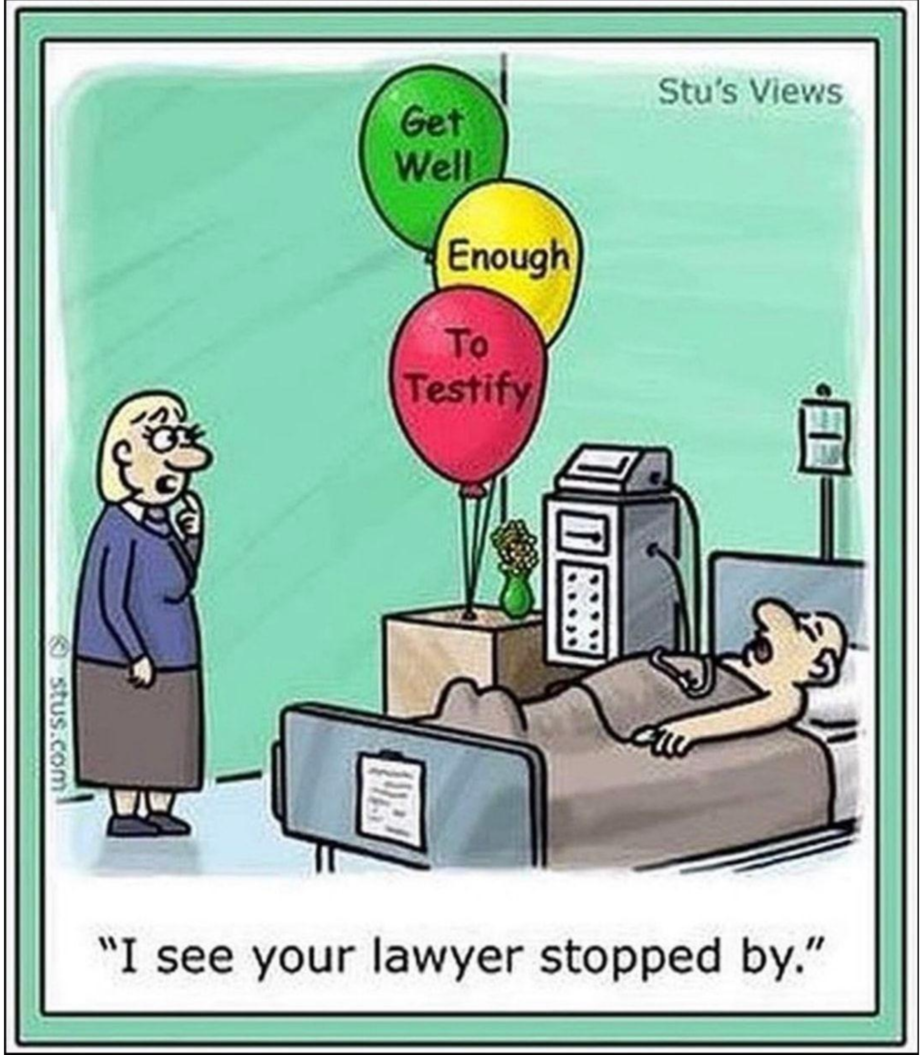
The Florida Bar's Standing Committee on Technology
Presents

How to Stop Hackers with Honey & Sand

Featuring:

Nick Lockard
CEO/CISO
Lockard
Managed Security Services Provider (MSSP) that specializes in defensive and offensive services.

Sponsored by LEGAL fuel
The Practice Resource Center of The Florida Bar



"I see your lawyer stopped by."

Topics

- Introduction
- Why You Should Care
- Risks
- Threats
- Common Security Controls
- Why they’re NOT enough
- Trojan and Ransomware Simulation Video
- The Good Stuff: Honey & Sand!
- Sandboxing
- HoneyTokens
- Defense-in-depth
- Lockard Services
- Q&A

OFFENSIVE® security OSCP

C|EH Certified Ethical Hacker

C|ND Certified Network Defender

CERTIFIED SECURITY ENGINEER

CERTIFIED SPECIALIST metasploit® pro

CompTIA Security+™ CERTIFIED

ace accredited configuration engineer

CompTIA Network+® CERTIFIED

CompTIA A+® CERTIFIED

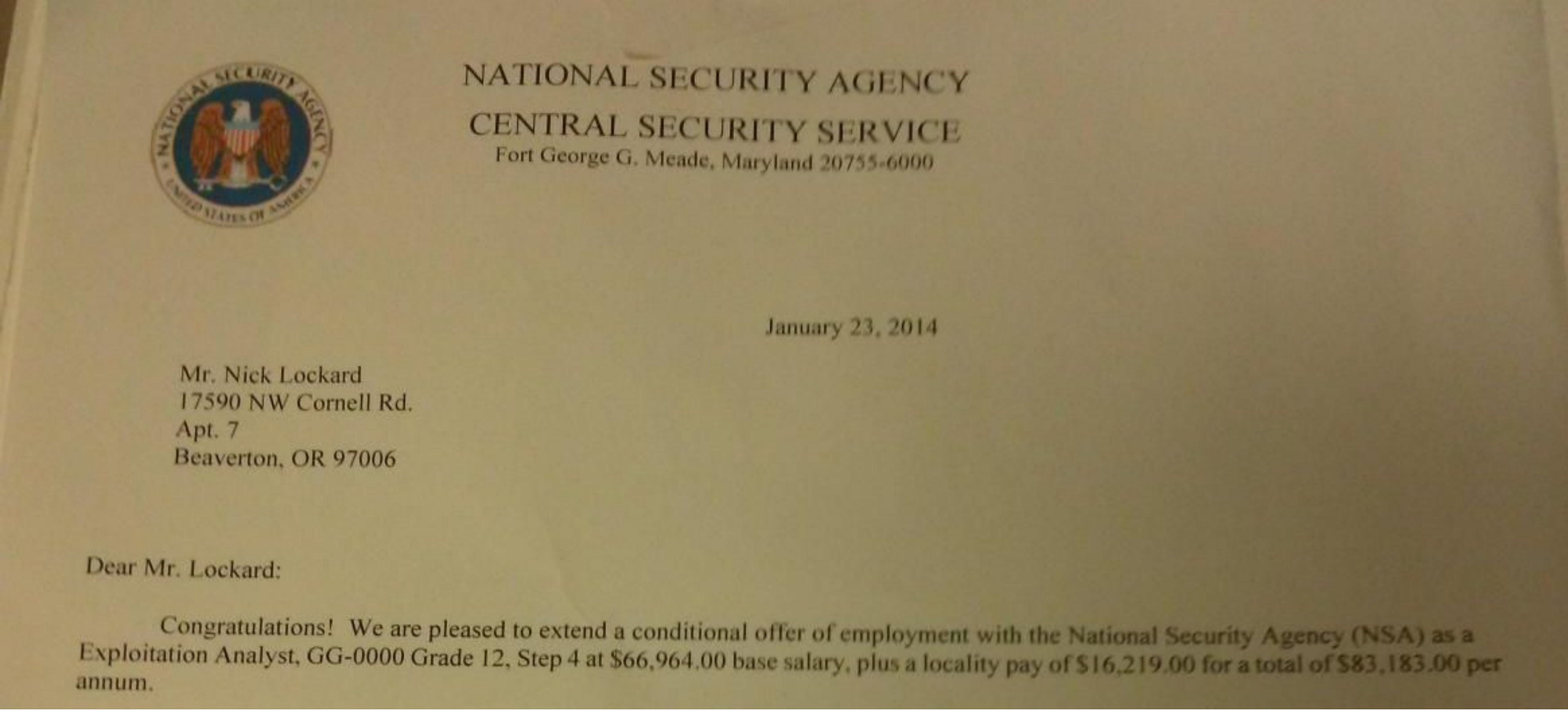
Nick Lockard

20+ years experience
Founder of Lockard, LLC.

Certified Ethical Hacker & OSCP
DOE, DOD, FBI, Intel, AWS, LinkedIn

Red, Purple, & Blue Team Operations
Security Engineering & Architecture

https://www.LockardSecurity.com
+1(833) LOCKARD



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland 20755-6000

January 23, 2014

Mr. Nick Lockard
17590 NW Cornell Rd.
Apt. 7
Beaverton, OR 97006

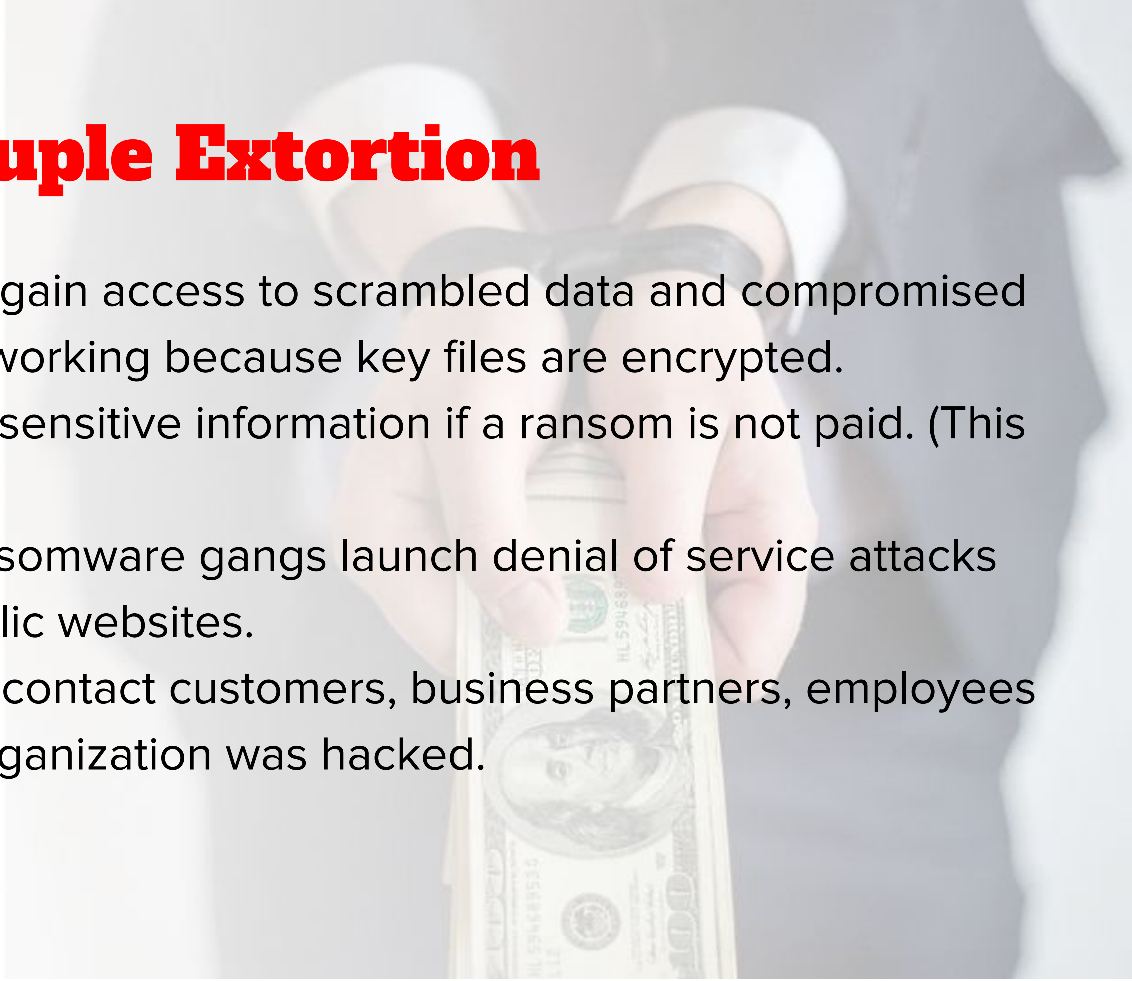
Dear Mr. Lockard:

Congratulations! We are pleased to extend a conditional offer of employment with the National Security Agency (NSA) as a Exploitation Analyst, GG-0000 Grade 12, Step 4 at $66,964.00 base salary, plus a locality pay of $16,219.00 for a total of $83,183.00 per annum.

Why You Should Care

- Reputation
- Everyone is a potential victim and humans are the top target
- 85% of beaches involved a human element
- 2020 - Average Ransomware Demand $847,000 (highest $30 million)
- 2021 - Average Ransomware Demand $5.3 million (+518%) (highest $50 million)
- Pegasus Trojan (Hacking phones with no click / no interaction)

The Risk of Quadruple Extortion



1. **Encryption:** Victims pay to regain access to scrambled data and compromised computer systems that stop working because key files are encrypted.
2. **Data Theft:** Hackers release sensitive information if a ransom is not paid. (This trend really took off in 2020.)
3. **Denial of Service (DoS):** Ransomware gangs launch denial of service attacks that shut down a victim’s public websites.
4. **Harassment:** Cybercriminals contact customers, business partners, employees and media to tell them the organization was hacked.

Risks

1. Unauthorized Access
2. Denial of Services
3. Malicious Code
4. Improper Use
5. Scanning / Probing / Attempted Access

Threats

- Adware
- Backdoor
- BHO
- Botnet
- DDOS
- Crypto Miner
- Exploit
- Keylogger
- Malware
- Phishing
- Ransomware
- RAT
- Rootkit
- Spyware
- Trojan
- Virus
- Worm
- Zero Day

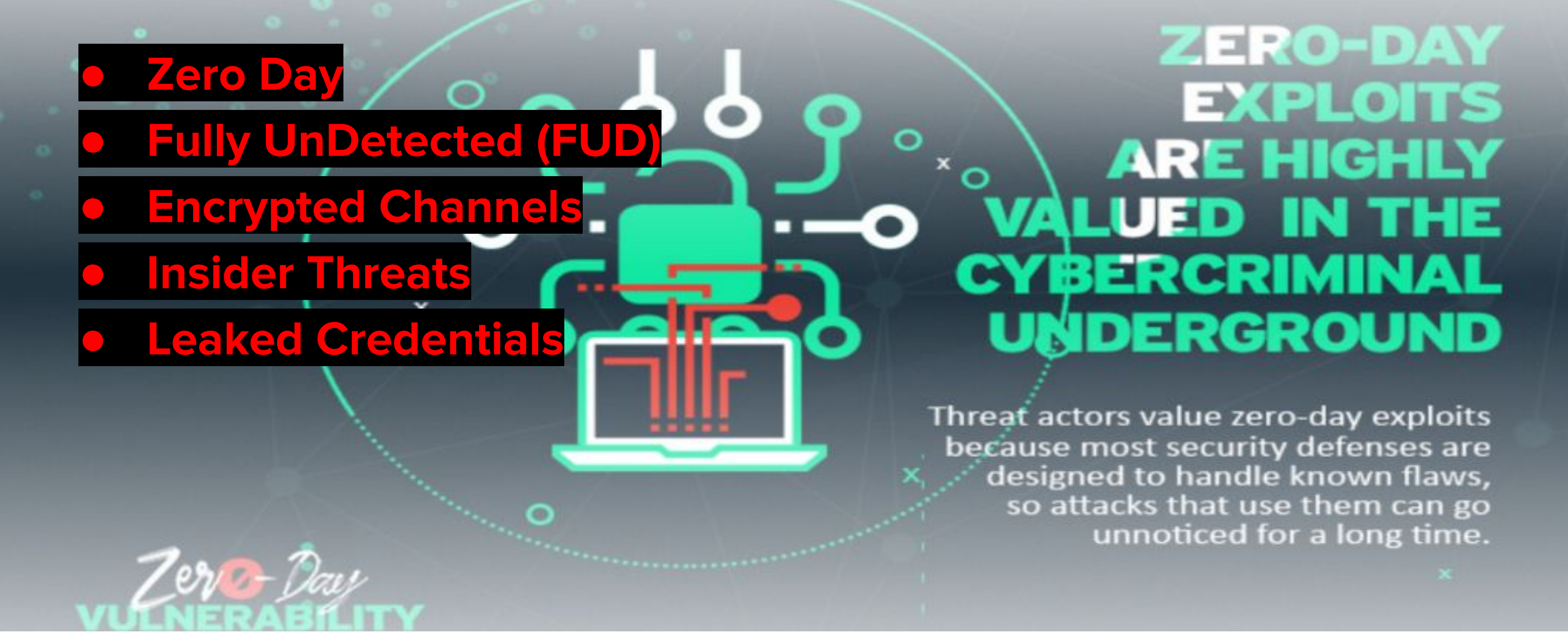
Common Security Controls

- Anti-Virus / Anti-Spyware / Anti-Malware / EDR
- Firewall / Intrusion Detection Systems
- Patching / Update
- Encryption
- Logging, Monitoring and Alerting
- Multi-Factor Authentication (2FA)
- Role Based Access Control (RBAC)
- Zero Trust
- Segmentation
- Locks / Motion Sensors / Lights / Badges / CCTV

MORE (Honey & Sand!) > all > some > one > none

Common Security Controls Are **Not Enough**

- Zero Day
- Fully UnDetected (FUD)
- Encrypted Channels
- Insider Threats
- Leaked Credentials

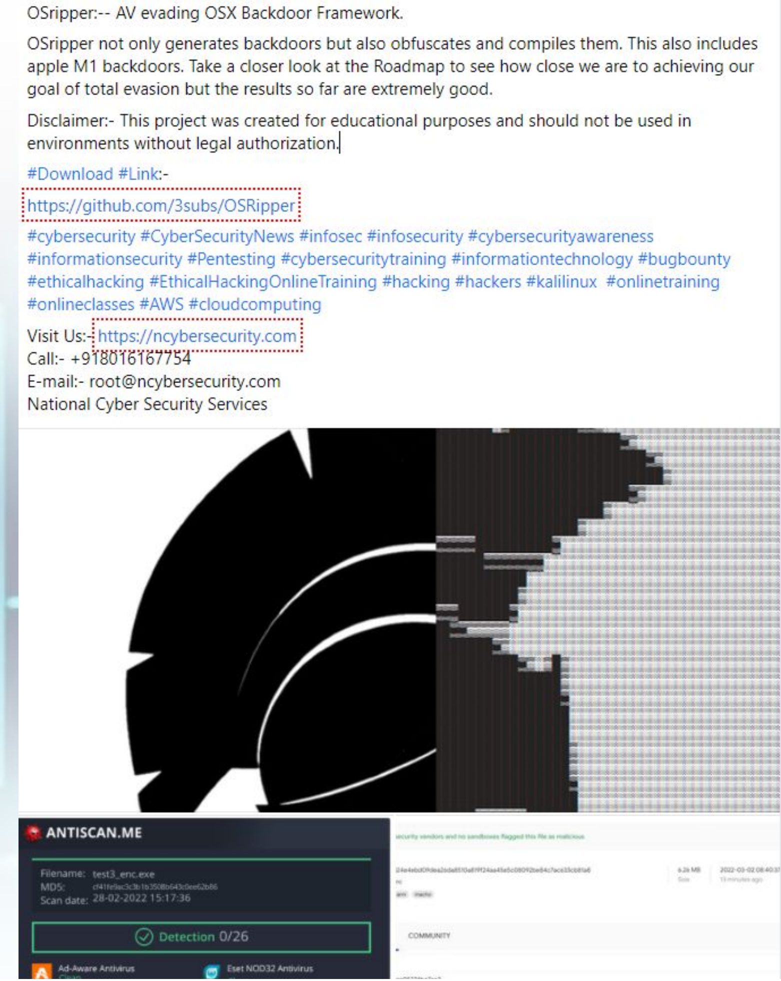


ZERO-DAY EXPLOITS ARE HIGHLY VALUED IN THE CYBERCRIMINAL UNDERGROUND

Threat actors value zero-day exploits because most security defenses are designed to handle known flaws, so attacks that use them can go unnoticed for a long time.

Zero Day For Apple's Mac

- https://github.com/SubGlitch1/OSRipper



OSripper:-- AV evading OSX Backdoor Framework.

OSripper not only generates backdoors but also obfuscates and compiles them. This also includes apple M1 backdoors. Take a closer look at the Roadmap to see how close we are to achieving our goal of total evasion but the results so far are extremely good.

Disclaimer:- This project was created for educational purposes and should not be used in environments without legal authorization.

#Download #Link:-

https://github.com/3subs/OSRipper

#cybersecurity #CyberSecurityNews #infosec #infosecurity #cybersecurityawareness #informationsecurity #Pentesting #cybersecuritytraining #informationtechnology #bugbounty #ethicalhacking #EthicalHackingOnlineTraining #hacking #hackers #kalilinux #onlinetraining #onlineclasses #AWS #cloudcomputing

Visit Us:- https://ncybersecurity.com
Call:- +918016167754
E-mail:- root@ncybersecurity.com
National Cyber Security Services

ANTISCAN.ME

Filename: test3_enc.exe
MD5: cf41fe9ac3c3b1b3508b643c0ee62b86
Scan date: 28-02-2022 15:17:36

Detection 0/26

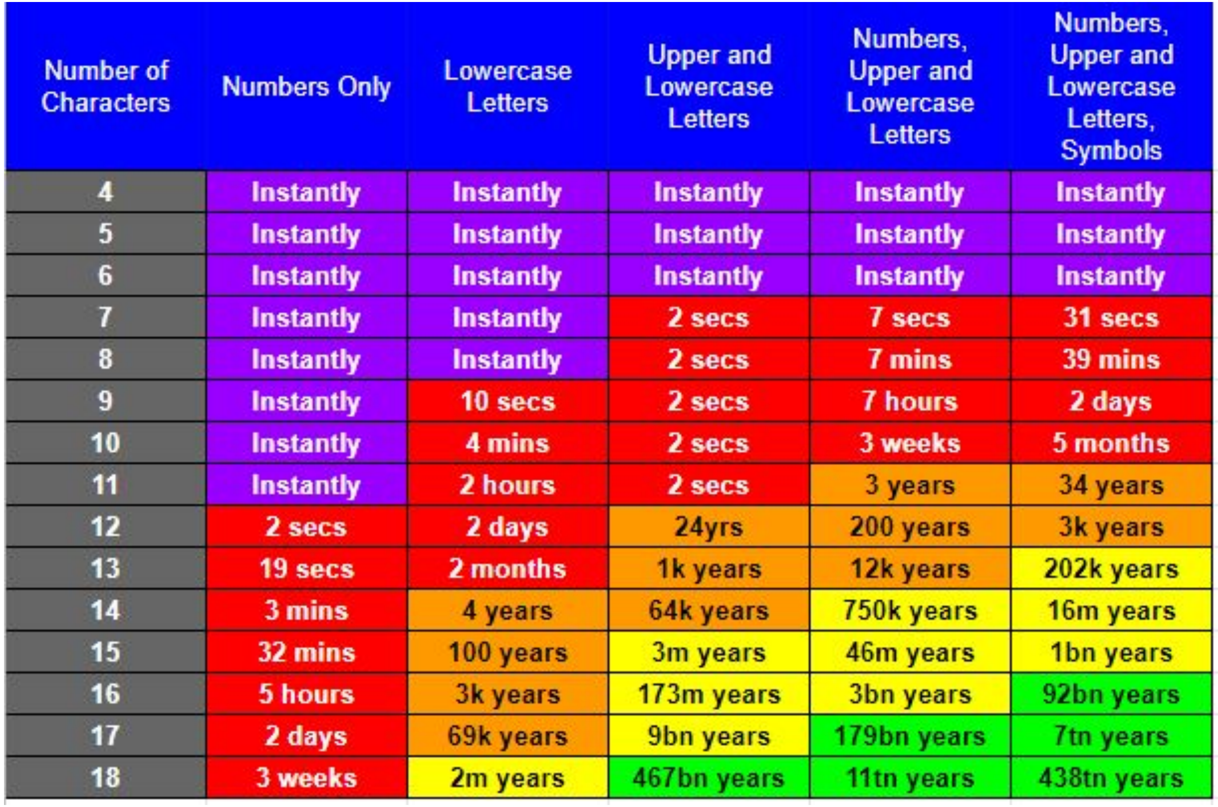
Ad-Aware Antivirus

Eset NOD32 Antivirus

security vendors and no sandboxes flagged this file as malicious

COMMUNITY

Time it takes a hacker to brute force your password in 2022



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 secs	7 mins	39 mins
9	Instantly	10 secs	2 secs	7 hours	2 days
10	Instantly	4 mins	2 secs	3 weeks	5 months
11	Instantly	2 hours	2 secs	3 years	34 years
12	2 secs	2 days	24yrs	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

www.LockardSecurity.com | +1 (833) LOCKARD

Protect Your Business | Protect Your Data | Protect Your Reputation

Trojan and Ransomware Simulation Video

https://www.youtube.com/watch?v=gARo-q7FTgA

The Good Stuff: Honey & Sand

- Sandboxing
- HoneyTokens
- HoneyPots
- HoneyNets

Sandbox

Sandbox 101

A sandbox is used to determine if something is bad.

Multiple types of Sandboxes:

- IP, URL and Website Detonation and Analysis
- File Detonation and Analysis

Advanced malware can detect certain types of sandboxes

Sandbox Tools

File

https://www.virustotal.com

https://www.joesandbox.com

https://antiscan.me

IP, URL and Website

https://www.urlvoid.com

https://www.ipvoid.com

https://www.scamvoid.net/

https://urlscan.io

https://pulsedive.com

Application

https://cuckoosandbox.org

CrowdInspect - https://www.crowdstrike.com/resources/community-tools/crowdinspect-tool

Demonstration of Sandbox

Upload file to VT - https://www.virustotal.com/gui/file/f6c3105a656571039e0224a7c73ddad2befaa00badf9dafd83d83a99eaaae824

Submit URL to VT - https://www.virustotal.com/gui/domain/lockard.it

Submit URL to URLVOID -https://www.urlvoid.com/scan/lockard.it/

Submit IP to VT - https://www.virustotal.com/gui/ip-address/8.8.8.8

Submit IP to IPVoid - https://www.ipvoid.com/ip-blacklist-check/

PulseDive: https://pulsedive.com/

URLScan: https://urlscan.io

Sandbox Limitations

Advanced Malicious code (Malware, Viruses, Trojans, Ransomware, etc..):

- Can evade detection
- Detect if running in a Sandbox
  - Bad stuff happens in
    - 5mins
    - 10mins
    - After you reach “level 3” in the game
    - Type the word “thanks”
    - At midnight
    - Etc…
  - Check for type of Operating System, architecture, IP Address, software installed, etc…

HoneyPots

HoneyTokens & HoneyPots 101

HoneyToken:

https://canarytokens.org/generate

HoneyPots:

- ElasticHoney
- DCEPT
- VMCloak
- MongoDB-HoneyProxy

HoneyPots & HoneyNets

HoneyPot

A HoneyPot can be a vulnerable system, application and/or setting that is configured in such a way that an attacker is enticed to target it.

- https://www.honeynet.org/

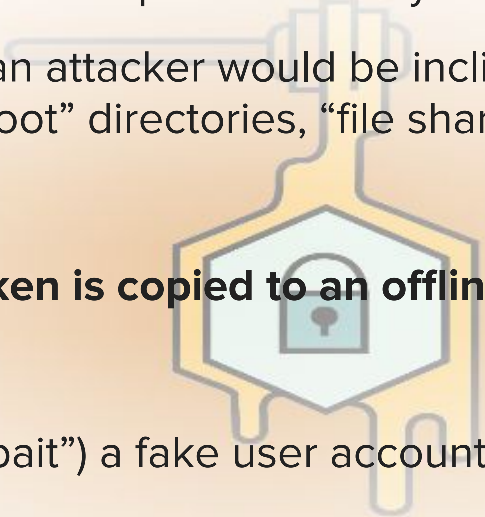
HoneyNet

A HoneyNet is a network that is set up to attract potential attackers and distract them from your production network. Consisting of a mix of HoneyPots and HoneyTokens

HoneyTokens Best Practices & Limitations

HoneyTokens should be used as “tripwires / booby traps” within your environment.

- Name them something an attacker would be inclined to open.
- Place them in “admin / root” directories, “file shares” and on servers.



Limitations - if the HoneyToken is copied to an offline system and opened.

HoneyToken Account (aka “bait”) a fake user account that looks normal and appears desirable to an attacker.

Demonstration of HoneyTokens

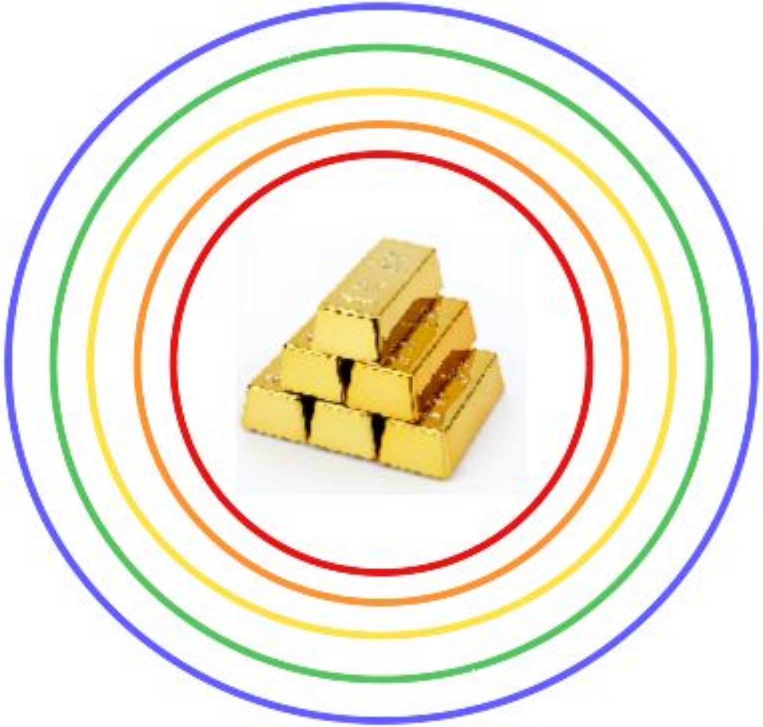
Step 1. Create HoneyToken - https://canarytokens.org/generate

Step 2. Open email - https://www.mailinator.com/v4/public/inboxes.jsp?to=lockard

Step 3. Open HoneyToken

Step 4. Upload to VT - https://www.virustotal.com/gui/home/upload

Defense-In-Depth



- Blue - Policy & Procedures
- Green - Physical Security
- Yellow - Network Security
- Orange - Endpoint Security
- Red - Application & Data Security

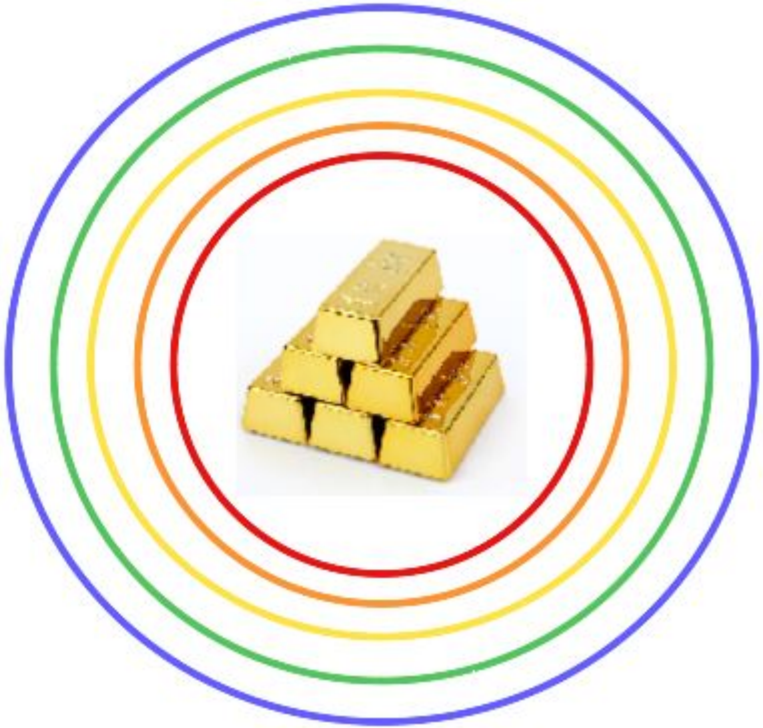
Bars of Gold = Crown Jewels

Crown Jewels - Classified Data

- Highly Confidential Data
  - PII - Personally identifiable information
  - PHI - Protected health information
  - SSN - Social Security Number
  - CC - Credit Card
  - IP - Intellectual Property
- Classified networks
- Classified systems / devices
- Email accounts
- SaaS accounts
- Social media accounts

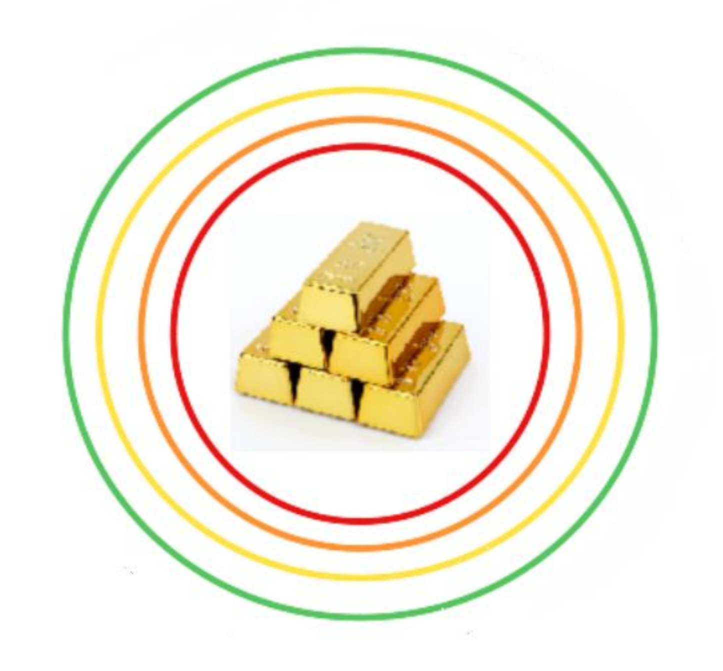
Blue - Policy & Procedures

- Risk Management
- Incident Response Management
- Supply Chain Management
- Audit and Assessment
- Training and Awareness



Green - Physical Security

- ID Cards / Badges
- CCTV
- Fences & Gates
- Locks
- Safes
- Alarms
- Motion Sensors



Yellow - Network Security

- Firewall
- Sandboxing
- Baseline Hardening
- IDS / IPS - Honey Pots
- VPN
- Monitoring and Alerting - Honey Tokens
- Vulnerability Assessment
- Cloud Security

Orange - Endpoint Security

- Baseline Hardening
- Application Allow listing
- Write and Read Protection
- Patching OS & 3rd Party Applications
- Endpoint Detection Response (EDR)
- Privilege Escalation
    - Least Privilege
    - Need-To-Know Principals
- Monitoring and Alerting - Honey Tokens

Red - Application & Data Security

- Privacy
- Classification
- Encryption
- Integrity
- Role Based Access Control (RBAC)
- Need-to-know
- Auditing
- Retention
- Destruction
- Availability
- Patching

Lockard's Here To Help, Call +1(833) 562-5273

A complimentary cybersecurity assessment to all Florida Bar members!

Email floridabar@lockardsecurity.com or give us a call today

Heavily discounted paid services to all Florida Bar members!

- Blue Team - 24x7x365 monitoring, alerting and incident response services
- Purple Team - Testing Blue Team Capabilities, Tools, and Processes
- Red Team - Ethical Hacking, Penetration Testing
- Tiger Team - B&E, lock picking, implants, rogue wifi, badge cloning, etc...

https://www.lockardsecurity.com/florida-bar/