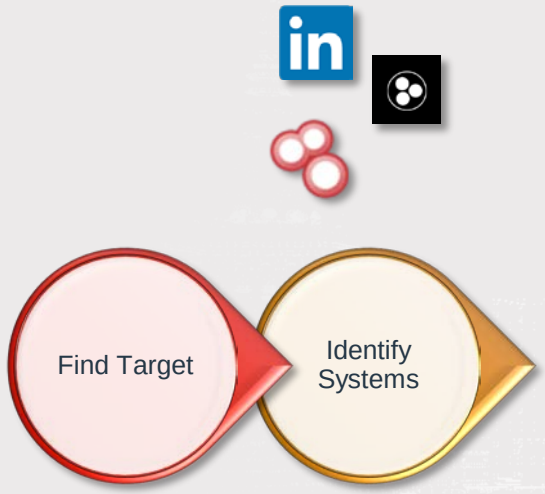
# What they do in Shadows.

*A look into hackers and cybercriminals, what's hot in their world and how that will impact yours.*

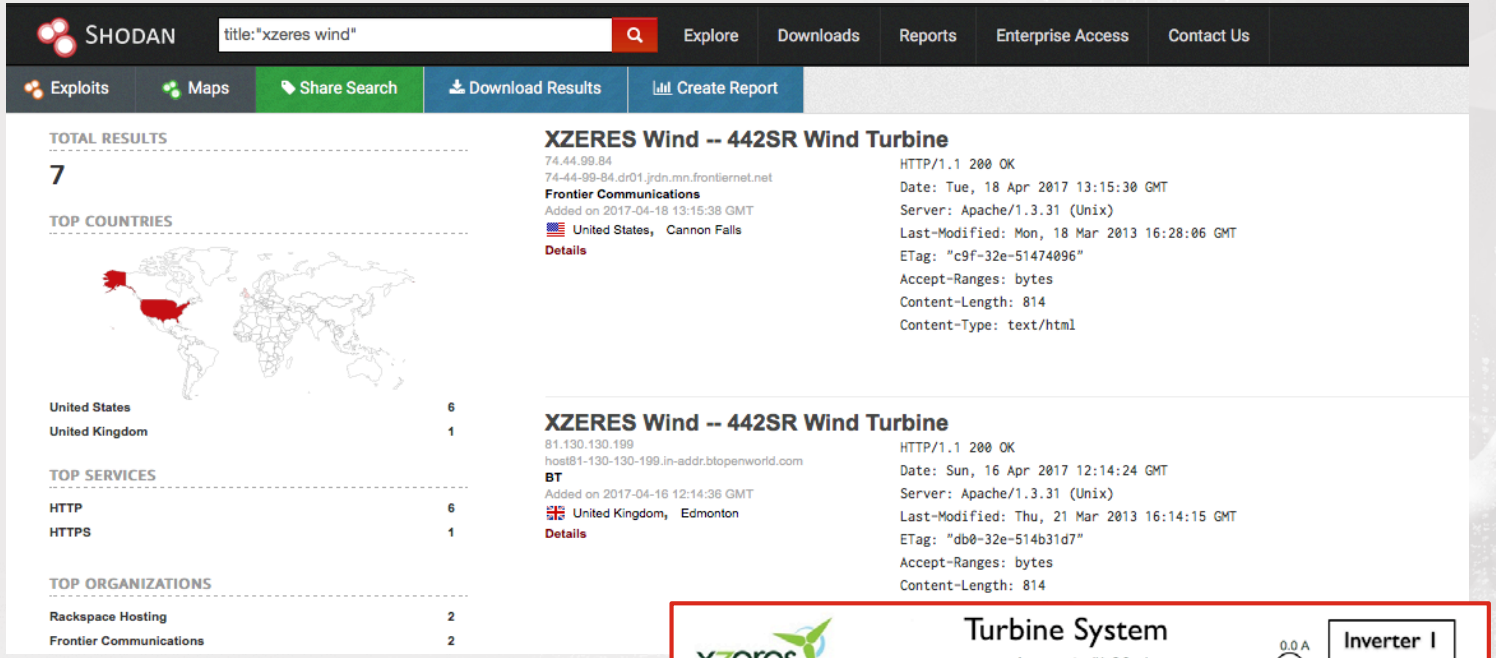
# Getting to Know You!

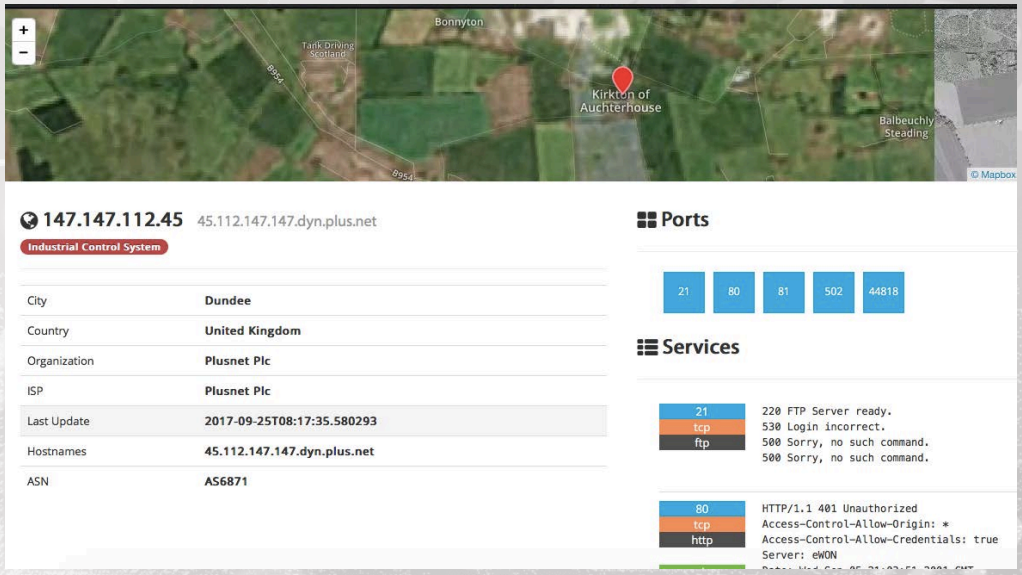
# H4cking Process

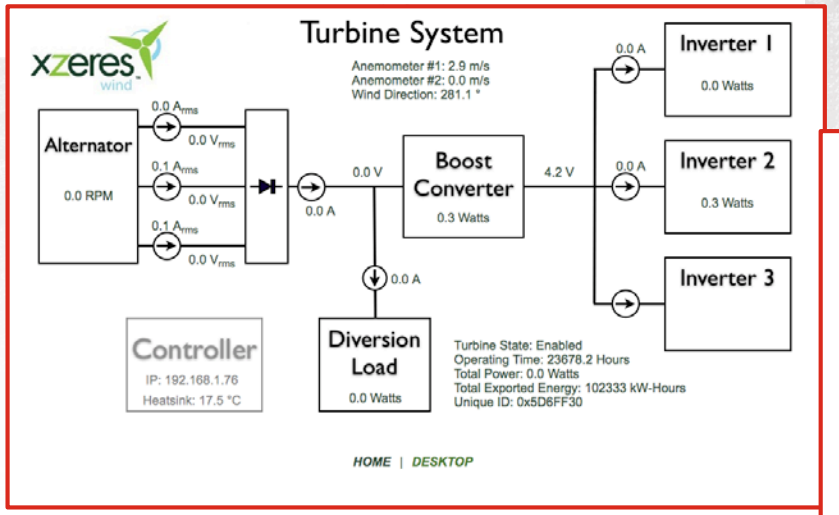


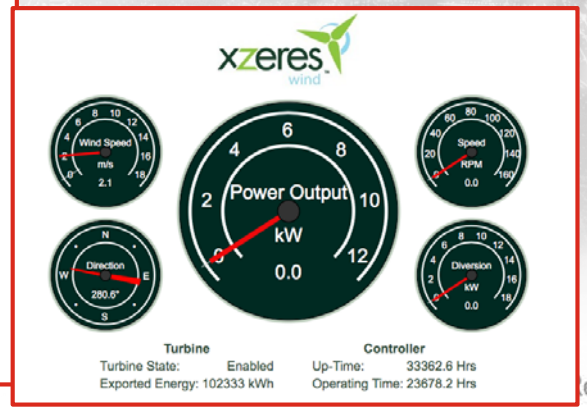

What you do.
What you have.
What you use.
Who you supply.

# Shodan.io

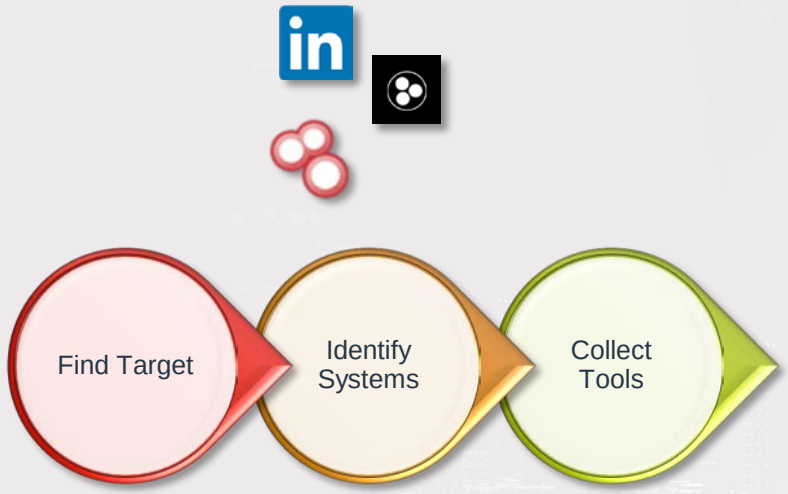


# H4cking Process




What you do.
What you have.
What you use.
Who you supply.

[ home ] [ private ] [ 0Day ] [ discount ] [ Get Gold ] [ platforms ] [ pentest ] [ hash ] [ search ] [ faq ] [ contact ] [ style ] [ Prices in Gold ] db: 32 706

Contact us:

[ authorization ] [ registration ] [ restore account ]

# 0DAY.today? Tor

0day Today is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals.
Our aim is to collect exploits from submittals and various mailing lists and concentrate them in one, easy-to-navigate database.
This was written solely for educational purposes. Use it at your own risk. The author will be not responsible for any damage. // r0073r

0day.today Available within TOR at http://mvfjfugdwgc5uwho.onion

## How to buy exploit? Two ways to buy required exploit. Currency, that we accept.

1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
2. Another way to buy exploits is to became 0day.today user, get 0day.today Gold and buy required exploit in our database.

bitcoin litecoin ethereum

We accept Crypto Currencies: [contact admin to find more]

Search: Search Extended search

## 0day Today Exploit Market and 0day Exploits Database

[ private ]

| ::DATE | ::DESCRIPTION | ::TYPE | ::HITS | ::RISK | | | | | ::GOLD | ::AUTHOR |
|---|---|---|---|---|---|---|---|---|---|---|
| 26-01-2018 | Twitter reset account Private Method 0day Exploit | tricks | 52 704 | | R | D | | √ | 0.216 | 0day Today Team |
| 07-01-2018 | Instagram bypass Access Account Private Method Exploit | tricks | 78 680 | | R | D | | √ | 0.216 | smokzz |
| 11-04-2018 | Hotmail.com reset account 0day Exploit | tricks | 20 782 | | R | D | | √ | 0.324 | 0day Today Team |
| 07-08-2018 | Facebook steal Group 0day Exploit | tricks | 22 918 | | R | D | | √ | 0.292 | 0day Today Team |
| 05-03-2019 | Snapchat takeover any account 0day Exploit | tricks | 8 135 | | R | D | | √ | 0.216 | 0day Today Team |
| 03-02-2019 | Tebilisim Remote File Read Vulnerability | php | 2 831 | | R | D | | √ | 0.054 | Zedros |
| 29-01-2019 | Mod_Security <= 3.0 Bypass XSS Payload Vulnerability | tricks | 2 645 | | R | D | | √ | 0.162 | champloo |
| 08-01-2019 | facebook - Grabbing permanent access token which Never expires of your accounts and pages | Android | 4 320 | | R | D | | √ | 0.216 | deep007 |

[ remote exploits ]

| ::DATE | ::DESCRIPTION | ::TYPE | ::HITS | ::RISK | | | | | ::GOLD | ::AUTHOR |
|---|---|---|---|---|---|---|---|---|---|---|
| 11-06-2019 | Webmin 1.910 - (Package Updates) Remote Command Execution Exploit | linux | 412 | | R | D | C | √ | free | AkkuS |
| 07-06-2019 | Exim 4.87 < 4.91 - (Local / Remote) Command Execution Exploit | linux | 593 | | R | D | C | √ | free | Qualys Corporation |
| 06-06-2019 | Inateck 2.4 GHz Wireless Presenter WP1001 Keystroke Injection Vulnerability | hardware | 443 | | R | D | C | √ | free | Matthias Deeg |
| 06-06-2019 | Inateck 2.4 GHz Wearable Wireless Presenter WP2002 Keystroke Injection Vulnerability | hardware | 377 | | R | D | C | √ | free | Matthias Deeg |
| 06-06-2019 | Logitech R700 Laser Presentation Remote Keystroke Injection Vulnerability | hardware | 300 | | R | D | C | √ | free | Matthias Deeg |
| 05-06-2019 | LibreNMS - addhost Command Injection Exploit | linux | 345 | | R | D | C | √ | free | metasploit |
| 05-06-2019 | IBM Websphere Application Server - Network Deployment Untrusted Data Deserialization | windows | 390 | | R | D | C | √ | free | metasploit |
| 04-06-2019 | Cisco RV130W 1.0.3.44 - Remote Stack Overflow Exploit | hardware | 428 | | R | D | C | √ | free | @0x00string |

[ local exploits ]

| ::DATE | ::DESCRIPTION | ::TYPE | ::HITS | ::RISK | | | | | ::GOLD | ::AUTHOR |
|---|---|---|---|---|---|---|---|---|---|---|
| 14-06-2019 | Aida84 6.00.5100 - (Log to CSV File) Local SEH Buffer Overflow Exploit | windows | 123 | | R | D | | √ | free | Nipun Jaswal |
| 14-06-2019 | CentOS 7.6 - ptrace_scope Privilege Escalation Exploit | linux | 170 | | R | D | | √ | free | s4vitar |
| 13-06-2019 | Pronestor Health Monitoring 8.1.11.0 - Privilege Escalation Vulnerability | windows | 105 | | R | D | C | √ | free | PovlTekstTV |
| 11-06-2019 | ProShow 9.0.3797 - Local Privilege Escalation Exploit | windows | 193 | | R | D | C | √ | free | Yonatan_Correa |
| 10-06-2019 | Ubuntu 18.04 - (bd) Privilege Escalation Exploit | linux | 273 | | R | D | C | √ | free | s4vitar |
| 07-06-2019 | Vim < 8.1.1365 / Neovim < 0.3.6 - Arbitrary Code Execution Vulnerability | linux | 412 | | R | D | C | √ | free | Arminius |
| 07-06-2019 | Microsoft Windows - AppX Deployment Service Local Privilege Escalation (3) Exploit | windows | 535 | | R | D | C | √ | free | SandboxEscaper |
| 07-06-2019 | Nvidia GeForce Experience Web Helper - Command Injection Exploit | windows | 447 | | R | D | C | √ | free | Rhino Security Labs |

[ web applications ]

| ::DATE | ::DESCRIPTION | ::TYPE | ::HITS | ::RISK | | | | | ::GOLD | ::AUTHOR |
|---|---|---|---|---|---|---|---|---|---|---|
| 13-06-2019 | Sitecore 8.x - Deserialization Remote Code Execution Vulnerability | asp | 152 | | R | D | C | √ | free | Jarad Kopf |
| 12-06-2019 | FusionPBX 4.4.3 - Remote Command Execution Exploit | php | 202 | | R | D | | √ | free | Dustin Cobb |
| 11-06-2019 | Liferay Portal 7.1 CE GA=3 / SimpleCaptcha API - Cross-Site Scripting Vulnerability | jsp | 173 | | R | D | C | √ | free | Valerio Brussani |
| 11-06-2019 | phpMyAdmin 4.8 - Cross-Site Request Forgery Vulnerability | php | 235 | | R | D | C | √ | free | Riemann |
| 11-06-2019 | WordPress Insert or Embed Articulate Content Plugin - Remote Code Execution Exploit | php | 255 | | R | D | | √ | free | xulchibalraa |
| 10-06-2019 | UliCMS 2019.1 Spitting Lama - Persistent Cross-Site Scripting Vulnerability | php | 174 | | R | D | C | √ | free | Unk9vvN |
| 07-06-2019 | Supra Smart Cloud TV - openLiveURL() Remote File Inclusion Vulnerability | hardware | 307 | | R | D | C | √ | free | Dhiraj Mishra |
| 06-06-2019 | Zimbra < 8.8.11 - XML External Entity Injection / Server-Side Request Forgery Vulnerability | jsp | 370 | | R | D | C | √ | free | k8gege |

[ dos / poc ]

| ::DATE | ::DESCRIPTION | ::TYPE | ::HITS | ::RISK | | | | | ::GOLD | ::AUTHOR |
|---|---|---|---|---|---|---|---|---|---|---|
| 05-06-2019 | Google Chrome 73.0.3683.103 - WasmMemoryObject::Grow Use-After-Free Exploit | multiple | 362 | | R | D | | √ | free | Glazunov |
| 31-05-2019 | Microsoft Windows Remote Desktop - BlueKeep Denial of Service Exploit | windows | 1 048 | | R | D | C | √ | free | Spencer |
| 29-05-2019 | Qualcomm Android - Kernel Use-After-Free via Incorrect set_page_dirty() in KGSL Exploit | Android | 507 | | R | D | C | √ | free | Google Security |
| 28-05-2019 | Spidermonkey - IonMonkey Unexpected ObjectGroup in ObjectGroupDispatch Operation | multiple | 410 | | R | D | C | √ | free | saelo |
| 28-05-2019 | Spidermonkey IonMonkey JS_OPTIMIZED_OUT Value Leak Exploit | multiple | 407 | | R | D | C | √ | free | saelo |
| 28-05-2019 | JavaScript V8 Turbofan Out-Of-Bounds Read Exploit | multiple | 447 | | R | D | | √ | free | saelo |
| 28-05-2019 | Cyberoam General Authentication Client 2.1.2.7 Server Address Denial Of Service Exploit | windows | 314 | | R | D | | √ | free | Victor Mondragón |
| 28-05-2019 | Cyberoam SSLVPN Client 1.3.1.30 Connect To Server / HTTP Proxy Denial Of Service Exploit | windows | 329 | | R | D | | √ | free | Victor Mondragón |

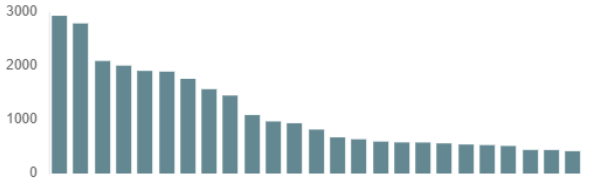
# VULDB

THE CROWD-BASED VULNERABILITY DATABASE

HOME ENTRIES PRODUCTS RISKS REFERENCES SEARCH SUPPORT LOGIN

## Product

### Entries »




Grouping vulnerabilities by *products* helps to get an overview. This makes it possible to determine an homogeneous landscape or the *most important hotspots* in heterogeneous landscapes.

### Type »

The *moderation team* is working with the *threat intelligence team* to *categorize software* that is affected by security vulnerabilities. This helps to illustrate the assignment of these categories to determine the *most affected software types*.

| Pos | Prod | Category | Link | Entries |
|---|---|---|---|---|
| 1 | Microsoft Windows | Operating System | microsoft.... | 2934 |
| 2 | Google Android | Smartphone Operating System | google.com | 2791 |
| 3 | Linux Kernel | Operating System | kernel.org | 2094 |
| 4 | Google Chrome | Web Browser | google.com | 2007 |
| 5 | Apple iOS | Smartphone Operating System | apple.com | 1909 |
| 6 | Mozilla Firefox | Web Browser | mozilla.org | 1895 |
| 7 | Microsoft Internet Explorer | Web Browser | microsoft.... | 1761 |
| 8 | Apple Mac OS X | Operating System | apple.com | 1569 |
| 9 | Adobe Acrobat Reader | Document Reader Software | adobe.com | 1451 |
| 10 | Adobe Flash Player | Multimedia Player Software | adobe.com | 1089 |
| 11 | Apple Safari | Web Browser | apple.com | 969 |
| 12 | Apple macOS | Operating System | apple.com | 936 |
| 13 | FFmpeg | Multimedia Processing Software | ffmpeg.org | 818 |
| 14 | PHP | Programming Language Software | php.org | 673 |
| 15 | Oracle MySQL Server | Database Software | oracle.com | 637 |
| 16 | Wireshark | Packet Analyzer Software | wireshark.... | 594 |

Information Technology Laboratory

# NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

## CVE-2015-3950 Detail

### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Current Description

Cross-site request forgery (CSRF) vulnerability in XZERES 442SR OS on 442SR wind turbines allows remote attackers to hijack the authentication of admins for requests that select a different default admin user via a GET request.

**Source:** MITRE

+View Analysis Description

## Impact

### CVSS v2.0 Severity and Metrics:

**Base Score:** 6.8 MEDIUM

**Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P) (V2 legend)

**Impact Subscore:** 6.4

**Exploitability Subscore:** 8.6

**Access Vector (AV):** Network

**Access Complexity (AC):** Medium

**Authentication (AU):** None

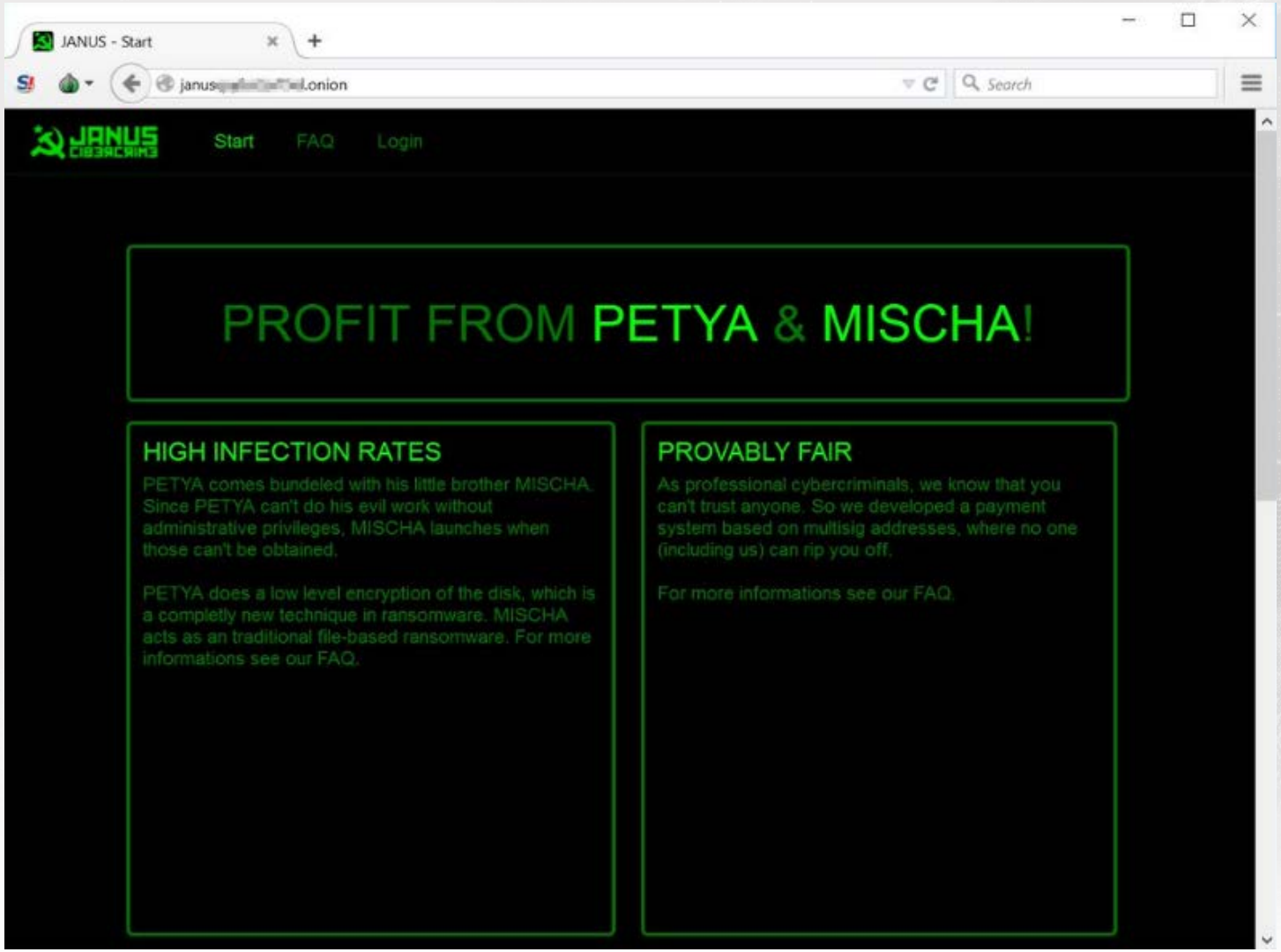
### QUICK INFO

**CVE Dictionary Entry:**
CVE-2015-3950

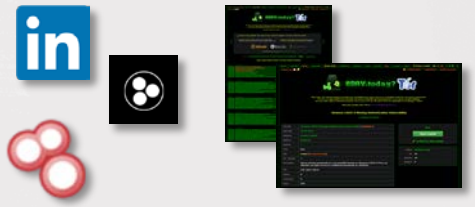
**NVD Published Date:**
06/05/2015

**NVD Last Modified:**
12/05/2016

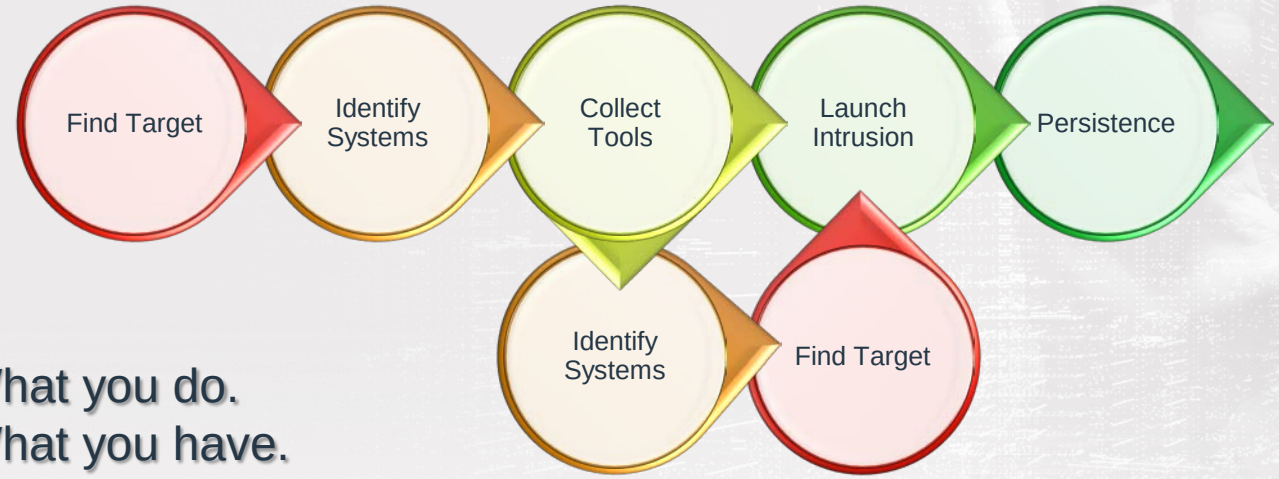
# RAAS



# H4cking Process



Live off the Land
Credentials are Key




What you do.
What you have.
What you use.
Who you Supply.

# Credentials

## Get your Credentials

- Hack You
- Hack a Site
- Buy Them.

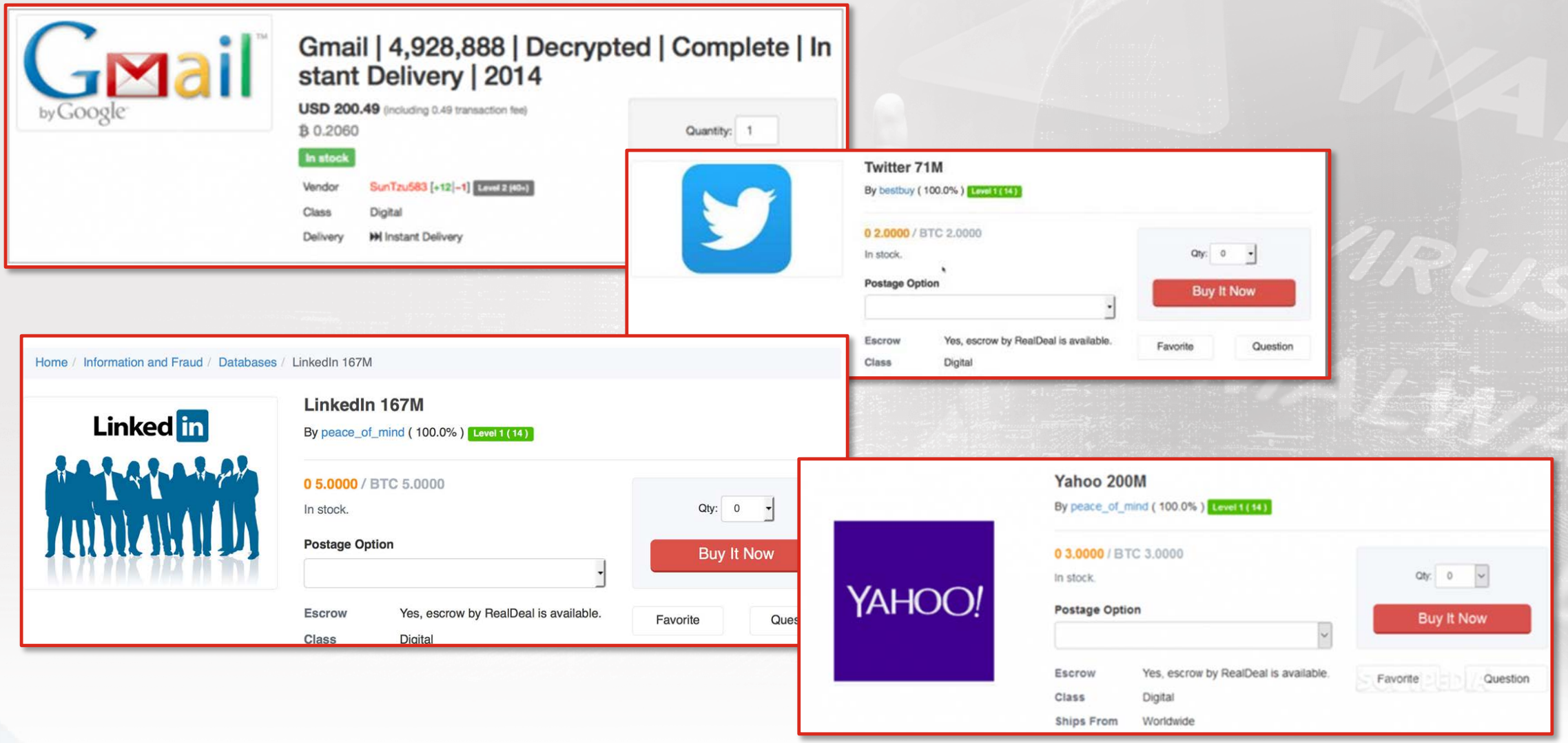
## Re-engineer your credentials

- 01 – 02
- Password – Pa55W0rD
- Facebook PW with FB

## Reuse your Credentials

- Social Media
- Email
- Banking / Financial
- Anything else

# Passwords for Sale



Have I Been Pwned: Che

https://haveibeenpwned.com/

Home | Notify me | Domain search | Who's been pwned | Passwords | API | About | Donate

# ';--have i been pwned?

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

bob@gmail.com pwned?

## Oh no — pwned!

Pwned on 150 breached sites and found 93 pastes (subscribe to search sensitive breaches)

### 3 Steps to better security

Start using 1Password.com

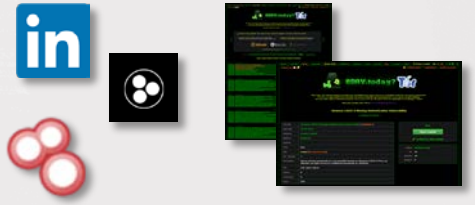

**Step 1** Protect yourself using 1Password to generate and save strong passwords for each website.

**Step 2** Enable 2 factor authentication and store the codes inside your 1Password account.

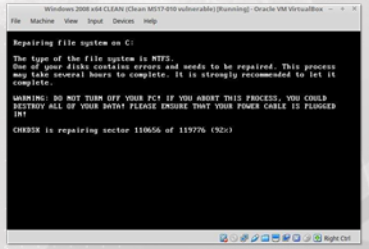
**Step 3** Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

# H4cking Process



Live off the Land
Credentials are Key



Find Target → Identify Systems → Collect Tools → Launch Intrusion → Persistence → Identify Value → Extract Value → Clean Up and Hide → Recycle / Resell

Identify Systems → Find Target

What you do.
What you have.
What you use.
Who you Supply.

Theft

Extortion

Fraud

Utility

# Cybercriminal Market Place

## CRIMESERVICE ENABLERS

**Quality Assurance**
Crypters / Packers
Scanners

**Hosting**
Infections / Drop Zones
Management

**Botnet Rentals**
Installs / Spam /
SEO / DDoS

**Money Mules**
Accounts Receivable

**Consulting**

## CRIMEWARE CONSUMERS

Bank Accounts

Credentials & Data

Digital Real Estate

**Victims**

**Criminal Organizations**

**Sales, Licensing, Maintenance**

**Affiliates**

Partnerships

## CRIMEWARE PRODUCERS

Exploits

Packers

Special Platforms

Mobile

Senior Developers

**Source Code**

*Copy & paste*

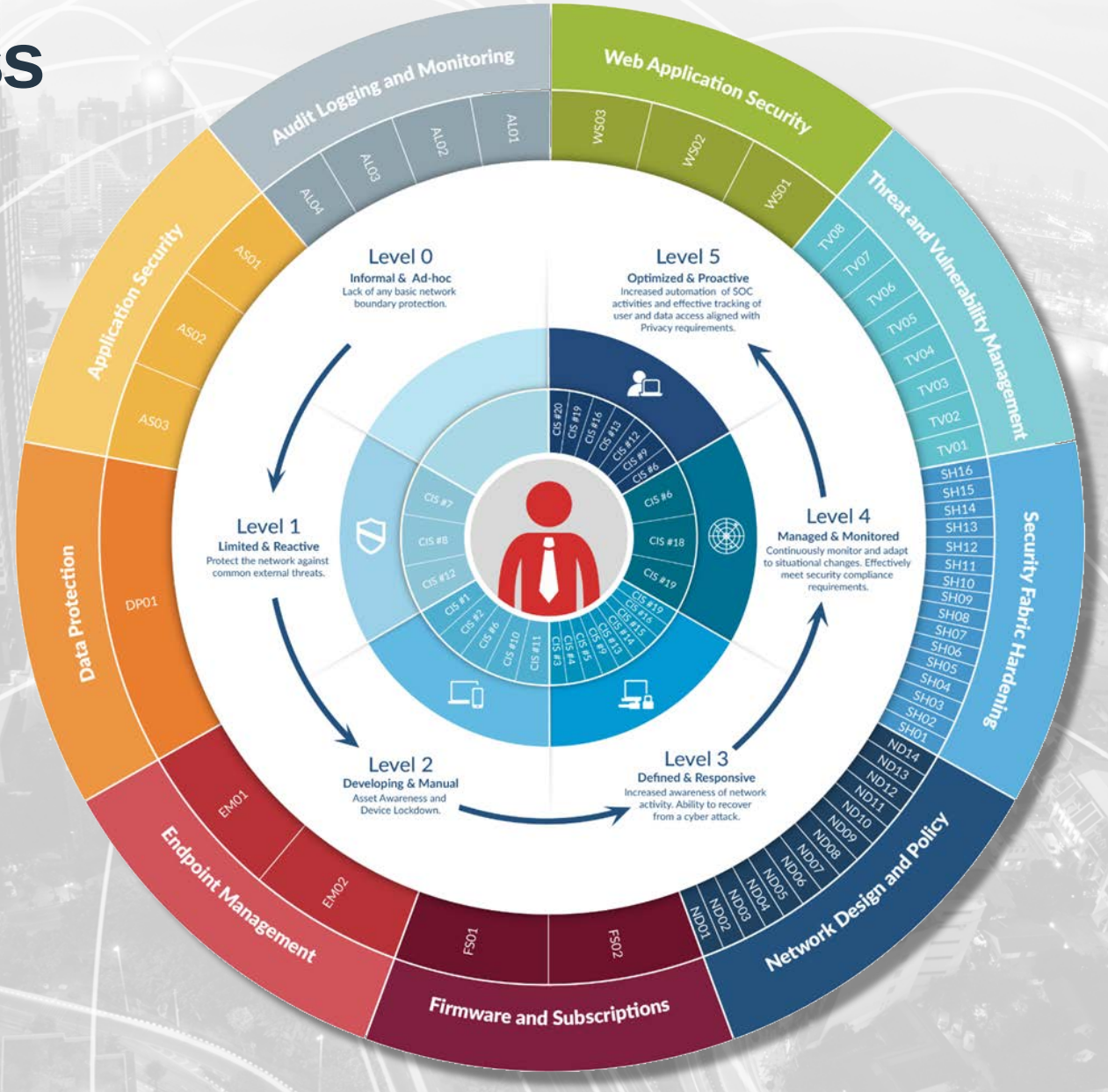
Junior Developers

**Affiliate Programs**
FakeAV / Ransomware / Botnets

# What Next for Security?

# Security As A Process

- Visibility
- Detection
- Control
- Reporting
- Measurement



# Cybersecurity 2020

- Hacking is a process. Defence should be too.
- People, Systems and Processes are targeted.
- Get the Basics right and build resilience from there.
- You can’t manage what you can’t see.
- Segment network and workloads.
- Integrated and automated gives the highest security.


FORTINET