



bit.ly/rgov

Everything is Hacked

“

"How I Learned to Stop Worrying and Love
Cybersecurity."

”

```
> cat /etc/identity  
EMAIL="nick@landeranalytics.com"  
PRETTY_NAME="Boxswapper"  
NAME="Nicholas Childs"  
FUNCTION0="Ethical Hacker"  
FUNCTION1="DEFCON 29 Speaker"  
FUNCTION2="Aeronautical Pentester"  
FUNCTION3="CISSP testing hopeful"  
FUNCTION4="CVE/NVD watcher"  
FUNCTION5="Server Mechanic"  
FUNCTION6="Kubernetes Wrangler"
```

Avionics Primer for Hackers DC29

“ This is first Markdown slidedeck so things are going to get scienced ”

- **1** Reported trends
- **2** MegaCorps gotta corp
- **3** Toys to break the world
- **4** Demo (hopefully)
- **5** Corrective Actions
- **6** Say Hello to RITA

- What is a hack
 - CIA TRIAD (Confidentiality, Integrity, Availability)
- What is a skid
 - Script Kiddie, a person who uses scripts to hack
- What is a vulnerability
 - A weakness in a system that can be exploited

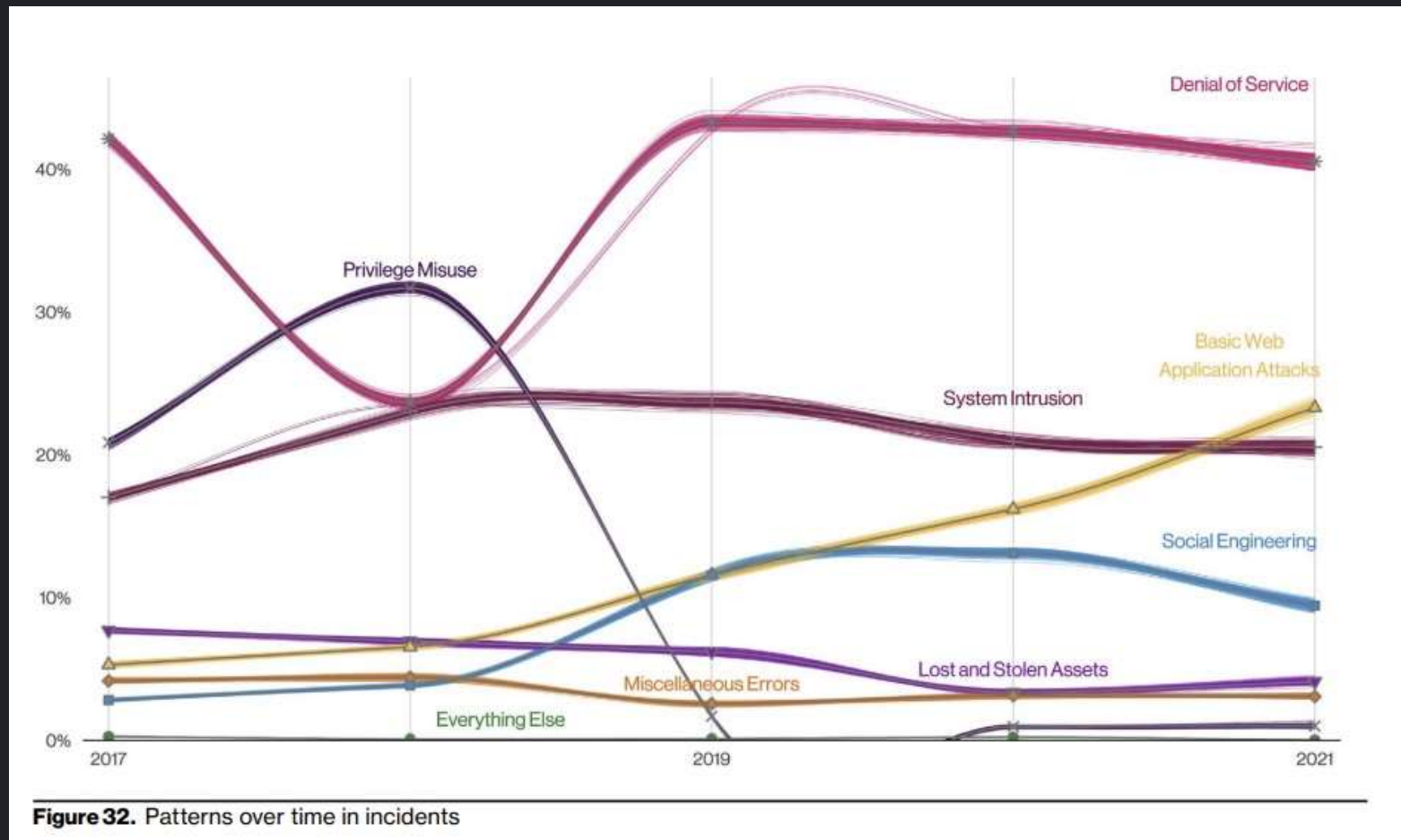
Reported Trends

- Verizon Databreach Investigation Report
- MITRE CVEs (Common Vulnerabilities and Exposures)
- NIST NVD (National Vulnerability Database)
- CISA Known Vulnerabilities and Exposures Catalog

Verizon DBIR Kurzgesat

- 2008 to present day
- Private & Public orgs
- VERIS (Vocabulary for Event Recording and Incident Sharing)
- 914,547 Incidents, 234,638 breaches = 8.9TB data

Reported Trends



pg. 23 Incident Classification patterns

Reported Trends

MITRE CVEs

Blue Team 's json files

- load into vulnerability scanners nicely
- 189,414 CVEs as of 2022-11-27
- Independent researchers, vendors, and other organizations submit CVEs
- POCs are common CTFs at competitions

Reported Trends

NIST NVD (National Vulnerability Database)

- 😡 Major source for automated Vuln management (SCAP)
- 👎 NIST standard the headache of administrators
- CVSS scoring system, Low, Medium High, critical

Reported Trends

CISA Known Vulnerability Exposures (KVE)

- Established w/ [Binding Operational Directive 19-02](#)
- 🏛️ Requirements for State and National Gov
- 💀 Drop dead date for CVEs
- 🚩 4 CVE fixes currently due 2022-12-19 (Always rolling)

Reported Trends

MegaCorps Gotta Corp

- ⚠️ Doing my best not to victim blame
- Features as a service, behind a paywall
- ❤️ Responsible disclosure is a thing
- IOT Fast and Cheap

Megacorps gotta Corp

Responsible Disclosure

- not all approved and public
- 0 Days out there in the wild
- companies not paying 💰 for bugs
- 🐛 resources not supporting Ethical hackers
- Hundreds Critical vulns released by [reputable hacker](#)






Megacorps gotta Corp

IOT Fast and Cheap

- IOT(S) port 515, 9100 tool called **PRET**

Megacorps gotta Corp

Toys to Break the World

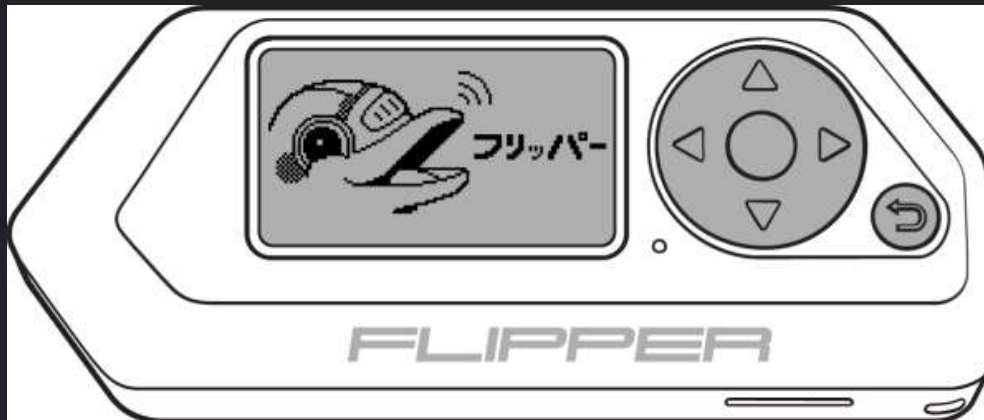
-  USB Rubber Ducky
-  flipperzero
-  HackRF
-  wifi pineapple
-  Shennina(23 Days ago)

Toys to break the world

USB Rubber Ducky



Flipperzero



Toys to break the world



HackRF



Toys to break the world



WiFi Pineapple

The screenshot displays the WiFi Pineapple web interface. On the left is a sidebar menu with the following items: Dashboard, Recon, Clients, Filters, Modules (expanded), PineAP (selected), Tracking, Logging, Reporting, Networking, Configuration, Advanced, and Help. The main content area is divided into two panels. The left panel, titled 'Configuration', contains several settings: 'Allow Associations' (checked), 'Log Probes' (checked), and 'Log Associations' (checked). Below these is a 'PineAP Daemon' section with a 'Switch' button and the text 'Enabled'. Further down are 'Capture SSIDs to Pool' (checked), 'Beacon Response' (checked), and 'Broadcast SSID Pool' (checked). At the bottom of this panel is a 'Save PineAP Settings' button. The right panel, titled 'SSID Pool', features a 'Refresh' button and a list of SSIDs: GuestWiFi, The Network, acme-guest, Concourse-B, Free WiFi, University Open, acme-floor3, Tenant 201, default, FreeWiFi, mobileAP, wireless, cablewifi, Home, and no_ssid. At the bottom of this panel are input fields for 'SSID', 'Add', and 'Remove'. Below the interface, the text 'Toys to break the world' is centered.

Toys to break the world



Shennina

“ Shennina is an automated host exploitation framework. The mission of the project is to fully automate the scanning, vulnerability scanning/analysis, and exploitation using Artificial Intelligence. Shennina is integrated with Metasploit and Nmap for performing the attacks, as well as being integrated with an in-house Command-and-Control Server for exfiltrating data from compromised machines automatically. ”

Toys to break the world

- Automated self-learning approach for finding exploits.
- Deception detection.
- Ransomware simulation capabilities.
- Automated data exfiltration.
- Heuristic mode support for recommending exploits.
- Out-of-Band technique testing for exploitation checks.
- Coverage for 40+ TTPs (Tactics Techniques procedures) within the MITRE ATT&CK Framework.

Shennina



Corrective Actions

Personal identity management "silos"

Password Manager

MFA whenever possible




!! keep it on your own hardware !!

Keep your crypto in the freezer

Corrective Actions

Meet RITA

(Real Intelligence Threat Analytics)

-  <https://github.com/activecm/rita>
-  <https://www.activecountermeasures.com/free-tools/rita/>
-  <https://www.activecountermeasures.com/getting-started-on-contributing-to-rita/>

Meet RITA

Threat Hunting

1. A trigger in the system leads to the formulation of a hypothesis.
2. The security team launches a deep dive to investigate the issue.
3. Extensive analysis and review of system logs, alert data, event data, network anomalies, endpoint alerts, and so on are reviewed to ensure thorough identification has been completed
4. The final step is resolution, after action report

Meet RITA



How RITA Works

- Beacon Detection: Identify signs of beaconing behavior in and out of your network.
- DNS Tunneling Detection: Identify signs of DNS-based covert channels.
- Identify Long Connections.
- View User-Agent strings.
- Deny-list Checking: Query blacklists to search for suspicious domains and hosts.

Meet RITA

Never enough Time

the-end