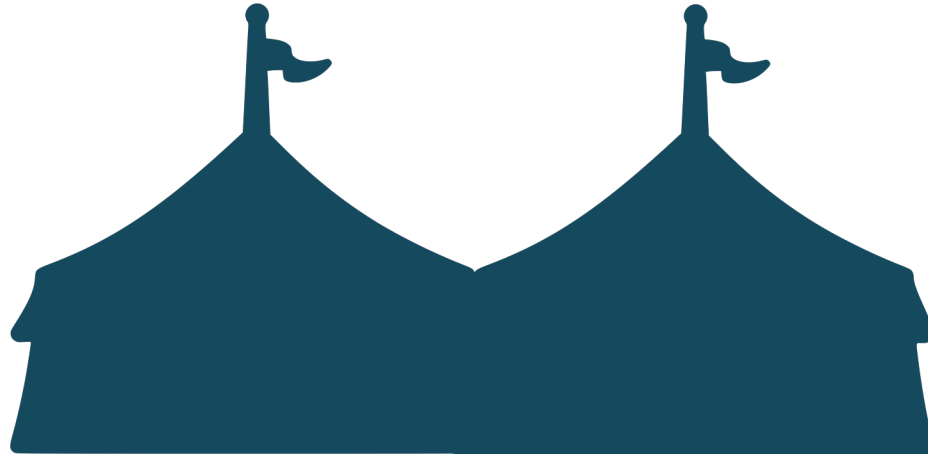




CIRCO v2

Cisco Implant Raspberry Controlled Operations



<https://circo.cc>

Hello, Virtual Friend

- My name is Emilio and I'm hacker 😁
- I like to play with packets, networks, electronics and 3D printers
- I presented security tools at various conferences (DEF CON, BlackHat Asia, AV Tokyo HIVE, Code Blue, SECCON, HITB, etc)
- Sorry, I'm not a native programmer or English speaker ☺
- UTC+9 (That's 16hr ahead of DEF CON)

Legal Disclaimer:



The tool is provided for educational, research or testing purposes.
Using this tool against network/systems without prior permission is illegal.

Radio waves are regulated per each country, before any radio wave transmission, make sure you comply within your country regulations (power, frequencies, bandwidth, etc.)

The author is not liable for any damages from misuse of this tool, techniques, code or radio frequency violations.

bla, bla, bla, bla...

Wait, what's CIRCO v1?

- ✓ Python 2
- ✓ Network implant using cheap hardware
- ✓ Behaves like a Cisco Switch (honeypot)
- ✓ Lure SecNetDevOps systems
- ✓ Exfiltrate obtained credentials via:
 - *ICMP*
 - *Traceroute*
 - *HTTP/HTTPS*
 - *DNS*
 - *NTP*
 - *Proxy*
 - *Wireless*
- ✓ Fully encrypted (avoid forensic)
- ✓ And more...



Got it, what's up with v2?

- ✓ Python 3
- ✓ Modular Code Structure
- ✓ MAC/IP Spoofing for exfiltration
- ✓ RTP/SIP (VoIP) call captures
- ✓ Support for *net-creds* tool to capturing credentials
- ✓ LDR (Light Dependent Resistor) for case-open alarm
- ✓ New exfiltration method (FM)
- ✓ Collect SIP Authentication
- ✓ New camouflage hardware
- ✓ Allow any TCP port for exfiltration
- ✓ SDR (Software Defined Radio) for exfiltration
- ✓ Improve Cisco IOS Honeypots (telnet, ssh, CDP and LLDP)



Honeypots (Cisco Services)

- Cisco CDP & LLDP Advertisement
(IP-Phone or Network Switch)
- Cisco SNMP Agent
- Cisco Telnet CLI (IOS 15.x)
- Cisco SSH CLI (IOS 15.x)
- Cisco TCP stack (fingerprinting)



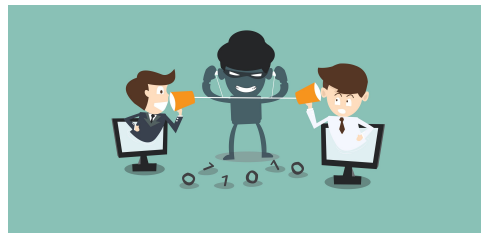
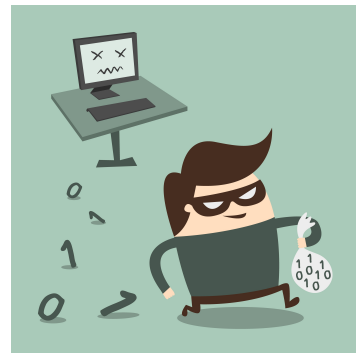
Exfiltration Formats

Honeypots

- Telnet
 - **t**,<username>,<password>,<src_IP>
 - **t,e**,<enable_password>,<src_IP>
- SSH
 - **s**,<username>,<password>,<src_IP>
 - **s,e**,<enable_password>,<src_IP>
- SNMP (v1/v2)
 - **p**,<community>,<src_IP>

Sniffed

- FTP, Kerberos, NTLMv1/2, SMTP, HTTP, etc.
 - **n**,<credential/hash>,<dst_IP>
- SIP
 - **v**,<hash>



Demo Labs

=

Demo Time!

Thank You!



(for watching)



Emilio#7052 (DEF CON Discord)



ekio_jp



<https://github.com/ekiojp/circo>



<https://circo.cc>