



Hackers are Humans too

Cyber leads to CI leads



Introductions

- [REDACTED]
- Cyber-counter intelligence
- My primary focus is MAKERSMARK (Russia)
- CSEC – Covert Network Threat (CNT) group
 - New name, same Cyber/CI group you know and love
 - Cyber and traditional CI sitting side by side
 - Focused on Foreign Intelligence, not Information Assurance



Goals

- How do we attribute cyber intrusion sets?
- How do we go beyond the hacking face of a CNE program?
 - Expose management structure, operators
 - Requirements, technological advances
- This presentation portrays only one method
 - Passive infrastructure tasking/contact chaining
 - Many other are available



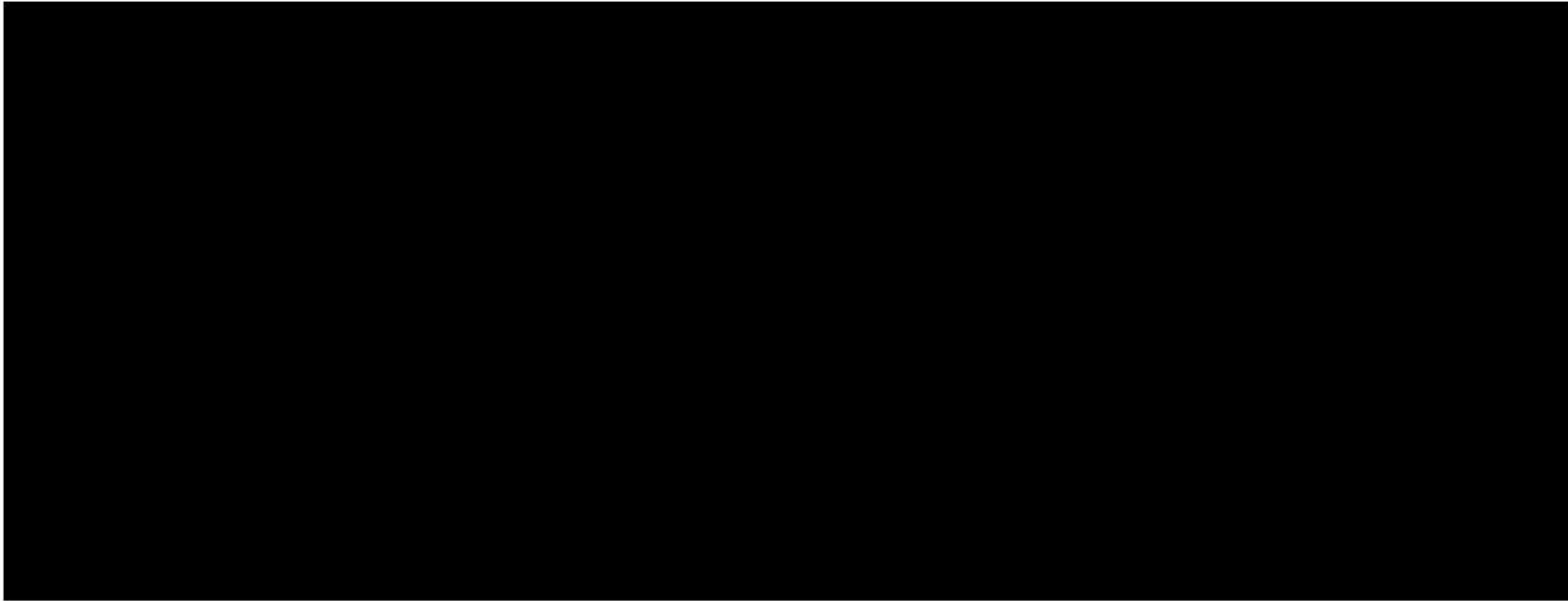
Initial Seed

- Infrastructure tasking
 - Mostly exposed through malware/content delivery
- Careful and manual monitoring of anomalous network sessions
- Nothing fancy
- Not Web 2.0, but it works



Overview

- MAKERSMARK
 - Misuse of Operational Infrastructure
 - Poor OPSEC practices





MAKERSMARK (Russian CNE)

Designed by geniuses
Implemented by morons

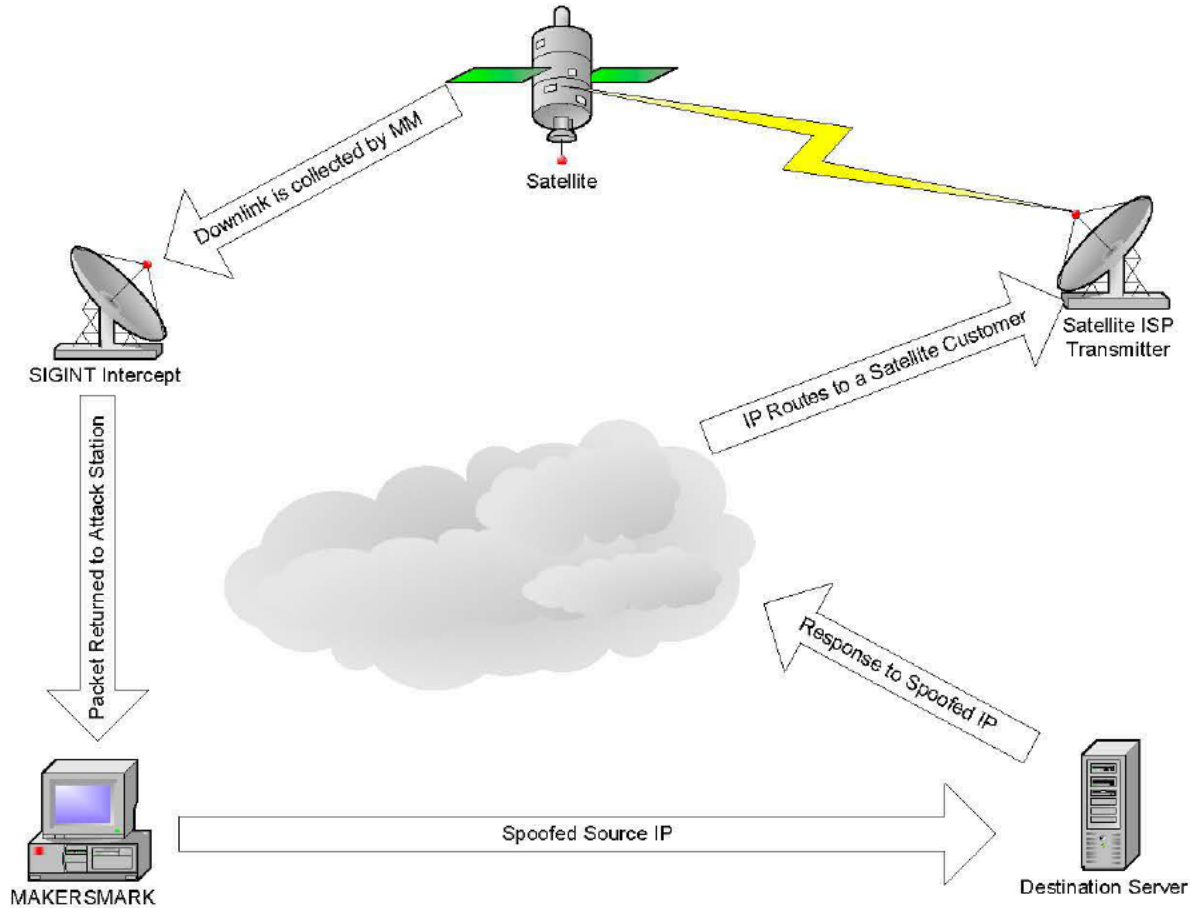


MAKERSMARK

- The MAKERSMARK less attributed (LA) systems are really well designed
- This has not translated into security for MAKERSMARK operators
- Personal browsing through LA systems
 - Workshops, ORBs, and controllers
- Development shop infected by crimeware
 - 4th party collection



MAKERSMARK: Less Attributed Overview





MAKERSMARK: Misuse of Infrastructure

- Less Attributable infrastructure used for highly attributable purposes:
 - Hosting implant callback servers
 - Live testing of new implant protocols
 - Collecting exfiltration
- This is not CNE best practices



MAKERSMARK: Misuse of LA Systems

- Personal Social Networking
 - Vkontakt
 - (mail/inbox/bk).ru accounts
- Personal Email
 - Webmail/POP
 - Personal retrieval through masquerading infrastructure
- Personal web browsing





MAKERSMARK: 4th party collection

- Implant development shop infected by GUMBLAR botnet
 - Crimeware
 - Sends pharmaceutical spam
- Exfiltration to Canadian “bullet proof” host
 - HTTP/FTP logins
 - Collection of MM operator browsing habits
 - MM LiveJournal accounts included in collection



Closing Remarks

- You have to keep an eye out
 - A lot of value can be lost by not following leads
 - Typically the window to exploit information is short
 - Knowing what to look for is half the battle
- These exploitation opportunities don't last forever
- As a CNE program matures, so will its OPSEC



Questions?



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu