TRANSGRESSION Overview for Pod58

S31177
7 Feb 2010

DERIVED FROM: NSA/CSSM 1-52
DATED 08 JAN 2007
DECLASSIFY ON: 20320108
Original:

Discover, understand, evaluate, and exploit foreign CNE/CNA exploits, implants, command & control and exfiltration.

Moving Forward:

Provide cryptanalytic exploitation support for Network Defense (NTOC and IAD), 4th Party SIGINT (S2, NTOC and TAO), and Cyber (TAO, RATWHARF) missions.
Personnel

- Branch Chief
- Team Lead/TD
- OTP CNE Co-Lead
- MAKERSMARK Lead
- BYZANTINE HADES Lead
- VOYEUR/Iran Lead
- Malware Lead
- Emerging Threats Lead
- MAKERSMARK, RDP Lead
- 1 CADP, 2 CMP (including DSD Integree), 1 RSE, 2 NIE, 2 STDP
Major Intrusion Set Efforts

- MAKERSMARK
  - Enable WALKERBLACK/RED exploitation/improve collection
  - CROWNROYAL, CROWNPRINCE, SHEPHERD, Zebedee

- BYZANTINE HADES
  - NetDef RDP exploitation
  - Trojan/beacon deobfuscation
  - MAVERICK CHURCH PPTP, POPROCKS

- VOYEUR (GHOSTRECON)
  - Victim Exfil
  - SSL Collection

- NIGHTTRAIN
  - Decryption and processing of TAO exfil and passive collect
  - SRE of malware

- SHADOWDRAGON
  - RDP and password recovery
  - FAA password recovery

- RECORDER
  - Processing and decryption of passive collect

- PLAIDDIANA/INCAADAM
  - Deobfuscation of passive collect

- TWEEZERS
  - Processing and decryption of passive collect

- SNOWGLOBE
  - Processing and decryption of passive collect

- WIDOWKEY/SUPERDRAKE
  - Future processing and decryption
  - Numerous other watchlist intrusion sets
  - Many one off customer requests – cyber cryptanalysis support
XKEYSCORE:
A Critical TRANSGRESSION Tool

- Over 50 daily workflows
  - SIGINT and POLARSTARKEY (NetDef)
- Fingerprints and Microplugins
- GUI Workflows and Webservice
Our Modernization Efforts

- XKS Webservice
- xksql and xkproc
- tfsql and tfproc
A Modernization Example

- Victim →
- LP →
- TAO Op →
- TUNINGFORK →
- TRANSGRESSION →
- SCISSORS →
- PINWALE and Cloud
Where does our data come from?

- XKEYSCORE
- TUNINGFORK
- TAO Direct
- NTOC Internal
- NTOC External
  - AFOSI/NCIS
  - FBI
  - Cyber Command

TOPSECRET//COMINT//REL TO USA, FVEY
What Kinds of Data?
(What is the plaintext)

- Command & Control
  - RDP, RAdmin \textit{(heavyweight)}
  - many home-grown \textit{(lightweight)}
- File Transfer
  - Actor $\rightarrow$ Victim \textit{(malware)}
  - Victim $\rightarrow$ Actor \textit{(exfil)}
- Email
- Credentials
What Kinds of Encryption?

1 - “Commercial”

- SSL/TLS
- SSH
- PGP
- PPTP
- RDP / RAdmin
What Kinds of Encryption?
2 – Other

- Block Ciphers (DES, 3DES)
- Stream Ciphers (RC4)
- Masking
  - short or long, fixed or variable
- Layered Encryption
Crypt Examples: Layered Encryption

- Byzantine Foothold
  - SSH
  - Mod DES

- Widowkey
  - Single Byte XOR
  - Fixed Key mask
  - 3DES
Crypt Examples: Setting Key

- Fixed (ADJUTANT VENTURE)
- From Message Header (RAPTOR ROLEX)
- From Packet Headers (RAPTOR JOY/SAD)
(U//FOUO) Who to Contact?

Email:

Wiki:
Encodings

- None (raw binary)
- base64
- Modified base64 (BYZANTINE RAPTOR)
  - A permutation of the 64 base64 characters
- HTML Character encoding (ADJUTANT VENTURE)
  - e.g., 0x1278cd = '\&#18;\&#120;\&#205'