



(S//REL)BYZANTINE HADES: An Evolution of Collection

[REDACTED] NTOC, V225

SIGINT Development Conference

June 2010



(S)What is BYZANTINE HADES?

- (S)BYZANTINE HADES = Chinese CNE
- (S)My Focus: Byzantine Candor





(S)BYZANTINE HADES Sets



(S)BYZANTINE CANDOR

- 80% of targeting against
 - DoD
 - Economic / Commodities (Oil Deals)
 - Current geopolitical / economic events



(S)BYZANTINE RAPTOR

- Resurfaced Summer '08
- 90% of activity targets DoD
- Has targeted Congress

(S)BYZANTINE ANCHOR

- Fairly universal targeting, but have observed
 - Weapon systems, information systems, NASA

(S)BISHOP KNIGHT

- Recent U.S. activity against (about 80%)
 - NASA, DoE, DoD, Defense Contractors

(S)BYZANTINE VIKING

- PLAN TRB

(S)MAVERICK CHURCH

- Formerly BISHOP



(S)BYZANTINE TRACE

- 95% of activity targets Ministry of Affairs / Defense
- Has targeted DoD, but not recently

(S)DIESEL RATTLE

- Within US: ISP's, defense contractors, government
- Japan



(S)BYZANTINE FOOTHOLD



- 50% of activity targets TRANSCOM
- 40% targets PACOM, U.S. Gov, defense contractors

(S)BYZANTINE PRAIRIE

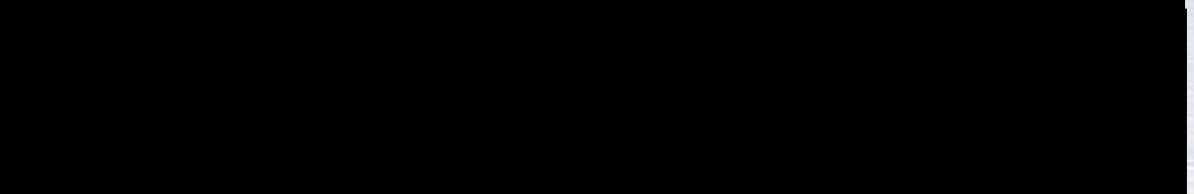
- Inactive since March 2008

(S)POP ROCKS

- 2009 Navy Router Incident
- Video Conference Providers

(S)CARBON PEPTIDE

(S)SEEDSPHERE (Not Assigned)





(S)BYZANTINE CANDOR

- (S)Formerly Titan Rain III
- [REDACTED]
- (S)Targeted E-mail Spearphishing tied to malware
- (S)Uses Dynamic DNS for mid-point C2 / Infrastructure; steganography to facilitate C2 (StegC2)



(U)Initial Searches

- (U)Reports
- (U)Task terms into SIGINT
 - Pinwale
 - XKeyScore
- (U)Link to other activity



(U)Analysis Tools

- (U)Crossbones
- (U)Domain and IP resolution
- (U)Google
- (U)TuningFork
- (U)Reports





(S//SI)Enabling Active Collection

- (S//SI)Pass IP to TAO
- (S//SI)Determine if host is vulnerable
- (S//SI)TAO Collection
- (S//SI)Review Collection



(U)And Analysis Reveals...

- (S)Hacker techniques
 - Not Sneaky
- (S)Attribution
 - Operate different from TAO
- (S)Exfiltration
- (S)Indications of future targets



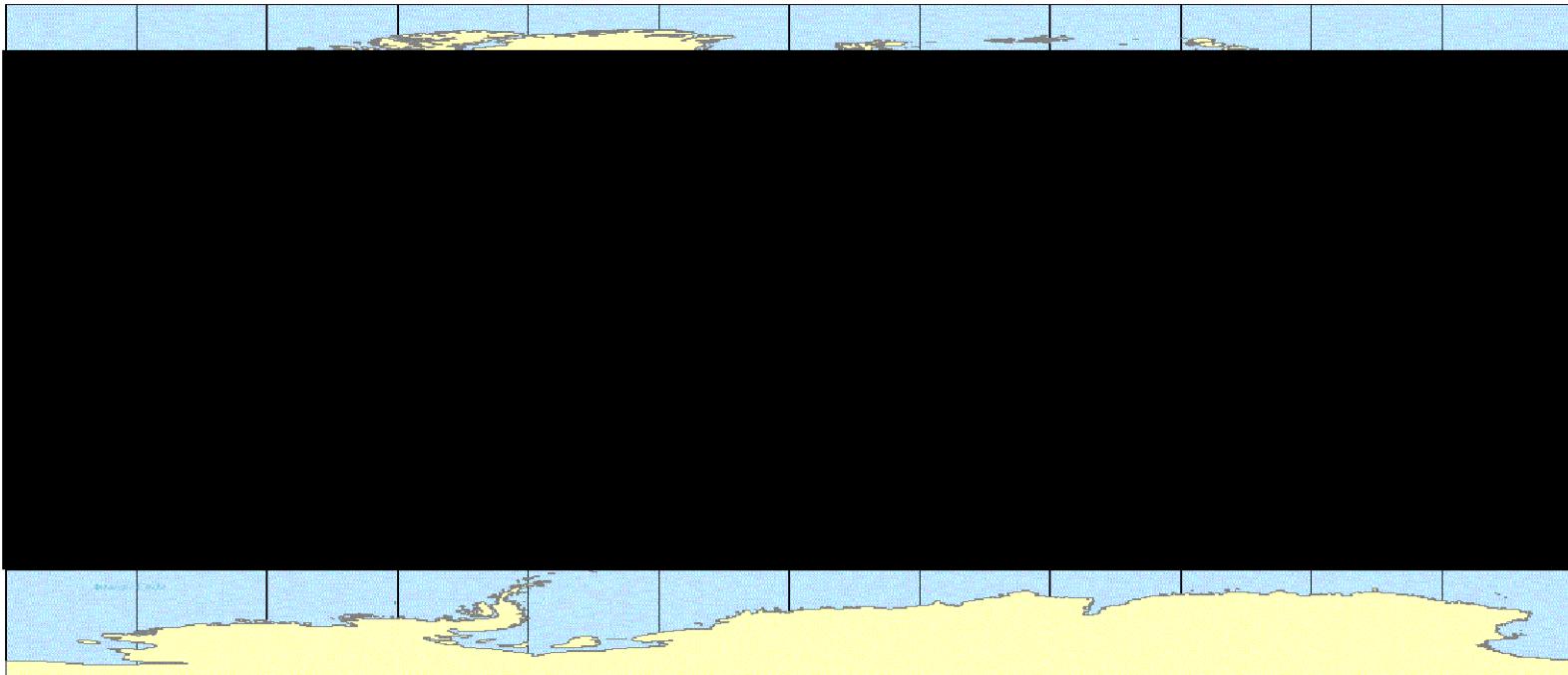
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



(S//REL) BYZANTINE CANDOR Infrastructure

Classification:

TOP SECRET//COMINT//REL TO USA, FVEY



BYZANTINE CANDOR C2 Hop Points

Plate Carrée Projection
Central Meridian: 0.00



Classification:

TOP SECRET//COMINT//REL TO USA, FVEY

As of 12 Aug 09 (8 weeks) ~350 observed

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



(S)Command and Control over FaceBook

The screenshot shows a Facebook profile page for a user whose picture is blurred. On the left, there's a sidebar with options like 'Upload a Picture' and 'Edit My Profile'. The main content area shows a post from a user named 'Jo Craw No.sorman1' with the ID '029228'. The post contains a URL: 'Face Meet5=615:<.555056Face Meet5:=069815/5<9'. Below the post are links to 'Comment', 'Like', and 'Share'. To the right of the post is a sidebar with advertisements for 'Become a Fan' and 'Alibaba.com'. At the bottom, there's a section about the wall, mentioning that posts are visible to anyone visiting the profile.

Victim malware posts to FaceBook page

BYZANTINE responds with implant commands



(TS)*Sigh*





(U)Success Stories – Ours and Theirs

- (S)TRANSCOM compromise by BC
 - Targeted two CDC's involved in development
 - Over 2500 files exfiltrated
 - Contractor's certificates
 - System-specific code
 - Program related documents
 - Admin passwords to GDSS Low-to-High guards
 - GDSS Message formatting



(U)Success Stories

- (S).gov networks
- (S)Significant World Events Targeting
 - Headlines
 - Shanghai World Expo
 - Any news that's fit to print!
- (S)Future Victims
 - Spear Phishing
 - Web C2
 - Victim research



(U)Knowledge Gaps

- (S)Additional hacker attribution
 - ArrowEclipse
- (S)How exfiltration is planned
- (S)Who is requesting the information
- (U)Overall picture



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

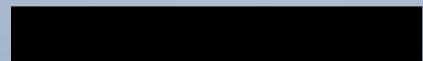


(U)Part 2

TAO...



(U//FOUO)Byzantine Candor: A TAO Success Story



Computer Science Development Program Intern

TAO\ Requirements and Targeting \ Cyber Counter-Intelligence

SIGINT Development Conference

June 2010

Derived From: NSA/CSSM

1-52

Dated: 20070108

Declassify On: 20350201



(U)It Begins...

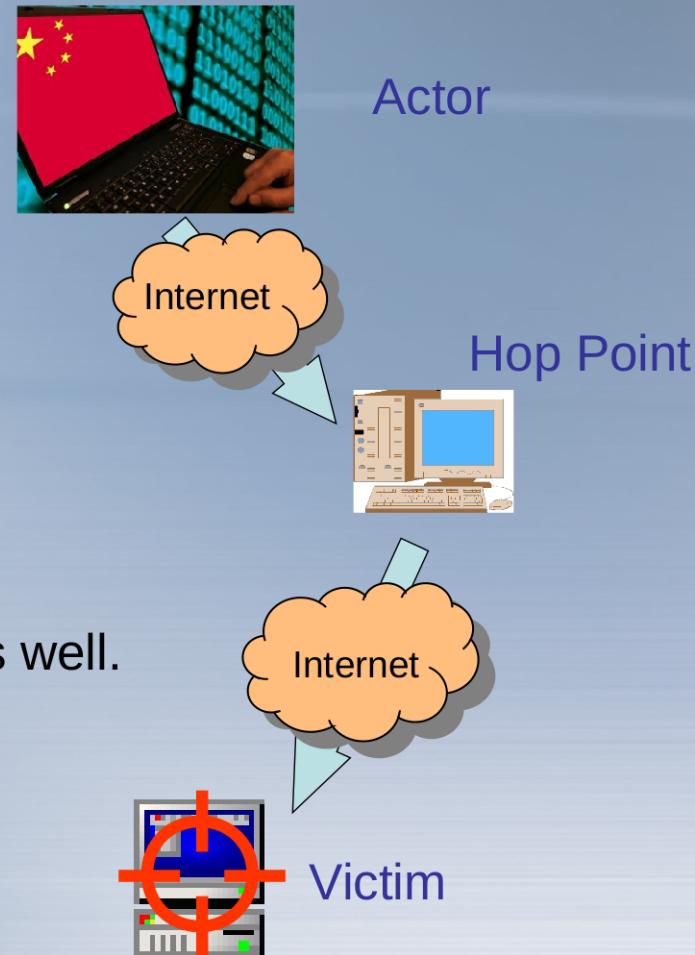
- (TS)Intrusion activity detected on DOD networks.
- (TS)NTOC requested TAO assistance in targeting foreign hosts involved in order to provide actionable intelligence to the CND community.





(S)What is a hop-point?

- (S)Hop-Point
 - Computer exploited by an actor
 - Generally of little Intelligence value
 - Used to connect to victims and conduct operations
- (TS)Majority of BC hop-points are US based.
- (TS)There are a number of foreign hop-points as well.
 - CCNE targets foreign hop-points





(S)Email Masquerades

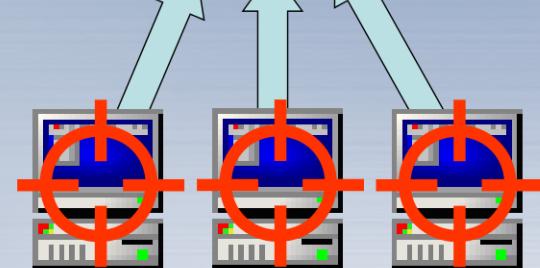
- (TS)Identification of hop points
 - Victim Callbacks
 - Other hop-points
- (TS)Types of Operations/Activities witnessed
 - Vulnerability/Port Scans
 - Remote Desktop Masquerades/ Email Masquerades
 - Spearphising
 - Remote Access tools
 - Altering callback domains
 - Personal web surfing (Checking e-mail, stock portfolio, surfing not safe for work material, etc)

Actor



Hop

Victims



LP



(U)It continues...

- (TS)We began conducting numerous operations on hop-points.
 - Exploiting new hosts
 - Collecting from existing hosts
- (TS)Started to put some pieces together and found the IP ranges the actors were coming from.
 - Unfortunately for us, the range is dynamic
 - Difficult to track
 - Difficult to target



(U)ARROWECLIPSE to the rescue

- (TS)ARROWECLIPSE

- Targeting the infrastructure of BC
- Exploited key routers in the ISP
- Gained access to billing and customer records.
- Attribute user accounts to IP addresses on a given date/time
- Ability to attribute a CNE event to a user account
- Attribute user account names to billing addresses
- Billing address is 3PLA

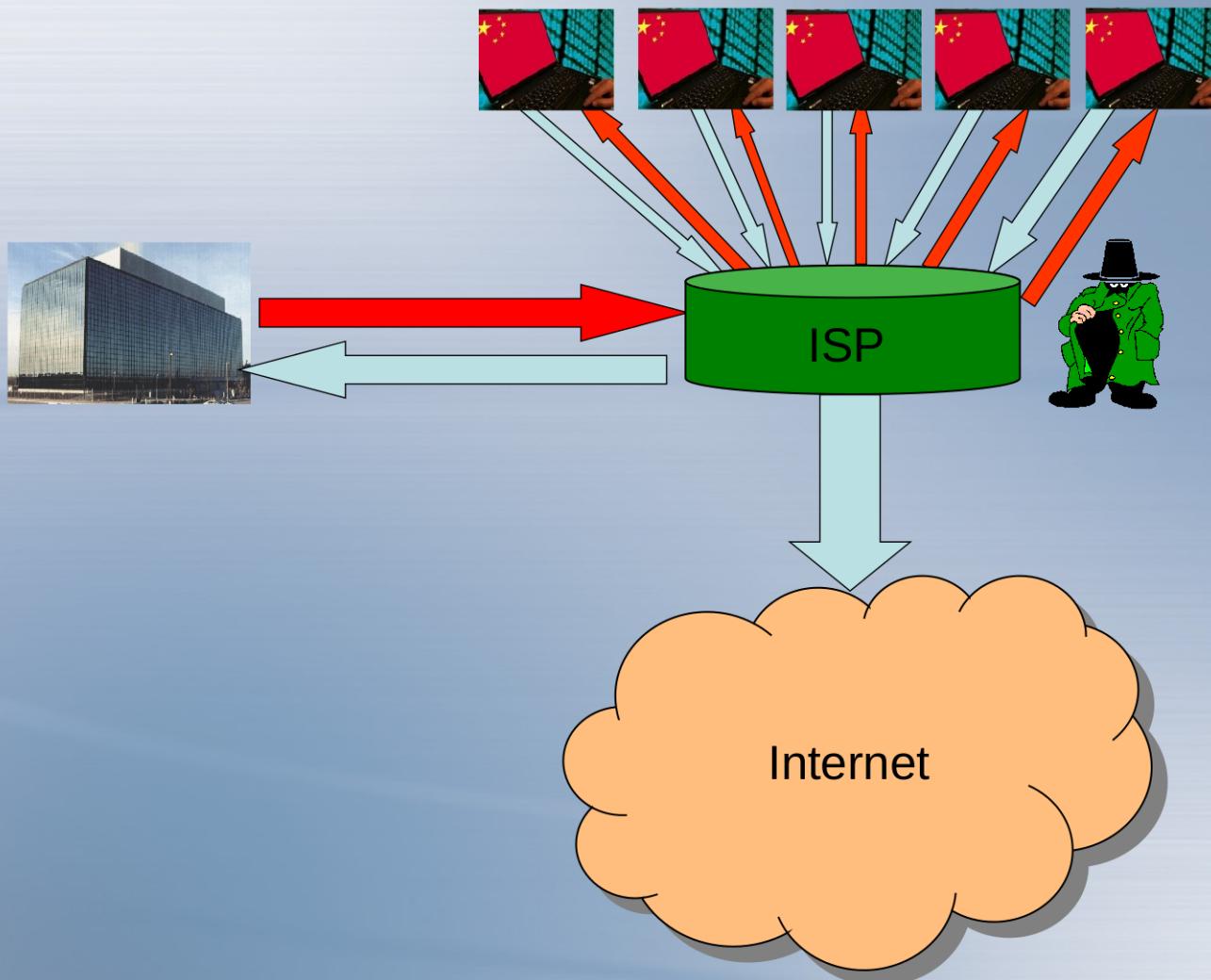


(U)What else can we do?

- (TS) So we can attribute CNE events to user accounts. What else can we do?
 - Using router accesses we can survey and capture remote desktop traffic exiting the source range.
 - New hop points!
 - Exploit the source network.
 - Man-in-the-Middle operation
 - We sit in the middle of the traffic, we can observe it and modify it.
 - Let's add something extra to the traffic.



(U)MitM





(U)Results

- (TS)Exploited 5 “computers” tied to known BC accounts.
 - “Computers” – 3 Virtual Machines, 2 Physical Machines
 - Exploited additional boxes not tied to known accounts.
- (TS)Exploiting the boxes was the easy part. Accessing the machines is a different story.
 - Lots of waiting
 - Lots of luck
 - Wading through “uninteresting” data
 - Pictures of family pets, old family photos
 - Wading through “interesting” but unrelated data
 - Pictures of PLA in uniform



(U)Accessing the machines

- (TS)Late October 2009
 - Finally interactively access an exploited virtual machine.
 - VM is associated with [REDACTED]
 - 3PLA
 - Probable CNE operations team lead
- (TS)Since then we have conducted numerous operations against the 5 source network machines
- (TS)Accessed a probable home/personal use box tied to [REDACTED]
 - Used work ISP credential for personal box



(U)Results

- (TS)Excellent sources of data
 - Used in interactive operations
 - CDCs, USG Entities, Foreign Governments, etc
 - Future target research
 - Bio's on senior White House officials, CDC employees, USG employees, etc.
 - Victim data
 - Source code and New tools
 - USB tools, exploits, remote access tools, etc.
 - Actor information
 - Email Addresses, Screen names,Pictures, etc



(TS)Cuteboy

- (TS) [REDACTED]
- (TS)CNE Actor
- (TS)Probable team lead
- (TS)Poor op-sec
- (TS)Implanted a VM associated with ISP account.
- (TS)Bonus: Implanted a physical box associated with ISP account, less frequently seen.

