An Easy Win:
Using SIGINT to Learn about New Viruses

Project CAMBERDADA
By [Redacted], I412 (IAD)
& [Redacted], V252 (NTOC)
Overall classification

TOPSECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
BRICKTOP (2009)

Kaspersky

RusComNet

Tascom

Rosoboronexport

Moscow Telecommunication Corporation (ComCor)

Institute of Information & Analytical Technology (IIAT)

Famatech

Comstar

Komet
Антивирус Касперского
Sample Email Received by an AV Vendor

PWZA20120510218350000197506

Good day,

A phishing scam file is attached for your analysis.
Zip file password = virus

The file tricks the user into giving her/his bank account credentials. This can be verified by clicking on the Sign In button.

FYI: https://www.virustotal.com/file/8fb6447fdc9cfe204cde...

Regards,
Francois Picard
www.NewRoma.net

Attachment: BMOFinancialGroup.zip
Work Flow
SIGINT brings in ~10 potentially malicious files per day for malware triage

Over 500 potentially malicious files collected since 2009

~ 50 CAMBERDADA signatures deployed to NIPRnet for alerting

9 domains mitigated
DNS Interdiction

9 domains under DNS Interdiction

Cloudshield intercepts the DNS request

Returns the address of a DoD listening post

Munged version of the request is sent out

DNS response is sent to a log
Current status

- CRN
  - SSO
  - Overhead
  - SCS
  - FORNSAT

IN L-C-2010-147 - Multi-Country: Computer Network Ops

Dozens of CADENCE selectors

PINWALE daily queries; EXIT4 models

MAILORDER
What else can we do?

- TAO can repurpose the malware
- Check Kaspersky AV to see if they continue to let any of these virus files through their Anti-Virus product
- Monitor the folks who provide the malware to see if they’re into more nefarious activity
- Establish automated reporting
More Targets!

Viritpro (Italy)
AVG (Czech)
k7computing (India)
Spy-Emergency (Slovakia)

fsb-antivirus (France)
F-prot (Iceland)

Norman (Norway)
Hauri (Korea)

Avira (Germany)
Nod32 (Slovakia)
Ahnlab (S Korea)

eAladdin (Israel)

Bit-Defender (Romania)
F-secure (Finland)

DrWeb (Russia)
Arcabit (Poland)
Novirusthanks (Italy)

Avast (Czech)
Checkpoint (Israel)
Eset (Slovakia)
Emsisoft (Austria)

Antiy (Chinese)