Knocking down the HACIENDA with TCP Stealth

Christian Grothoff
Actual work: Julian Kirsch

Technische Universität München

July 23, 2015

What is HACIENDA?

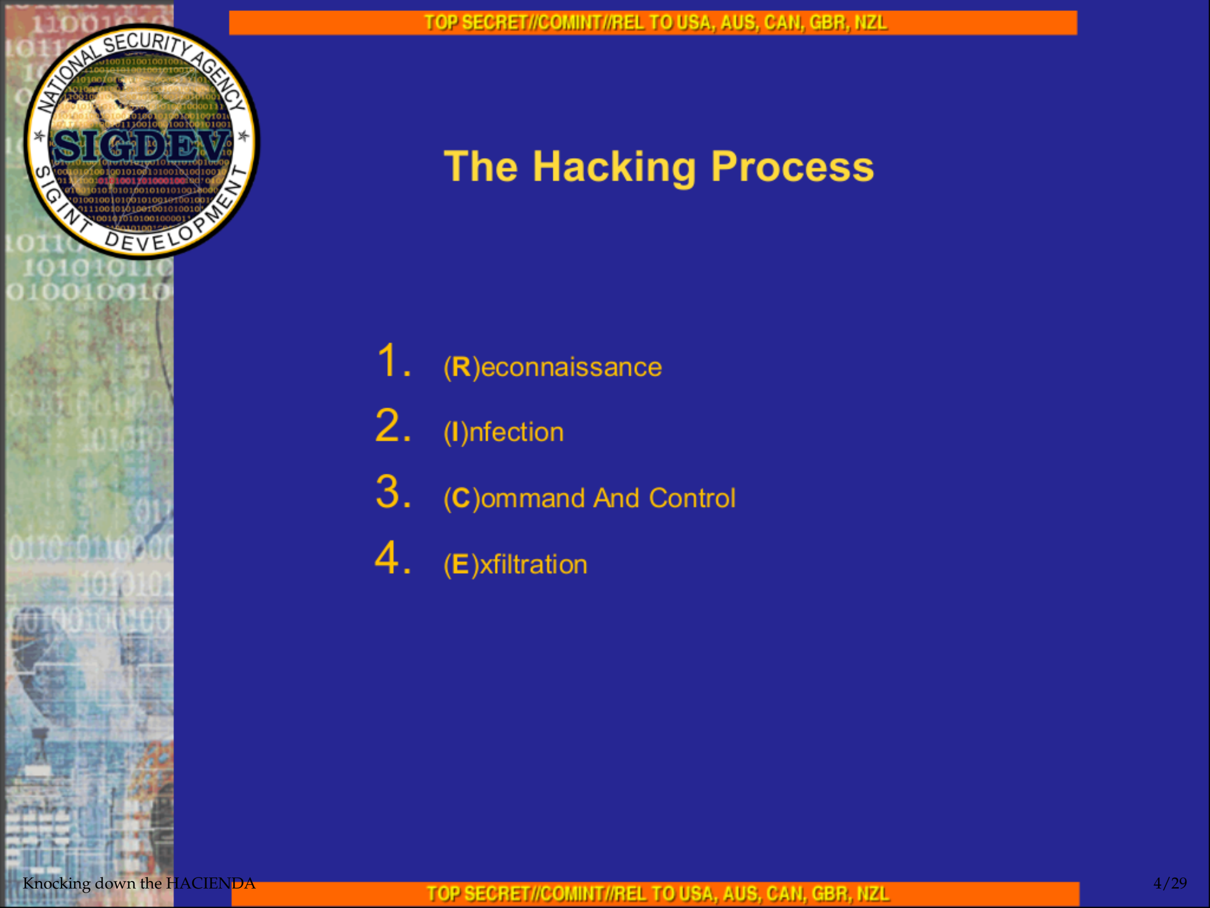
- Data reconnaissance tool developed by the CITD team in JTRIG
- Port Scans entire countries
  - Uses nmap as port scanning tool
  - Uses GEOFUSION for IP Geolocation
  - Randomly scans every IP identified for that country

How is it used?

- CNE
  - ORB Detection
  - Vulnerability Assessments
- SD
  - Network Analysis
  - Target Discovery

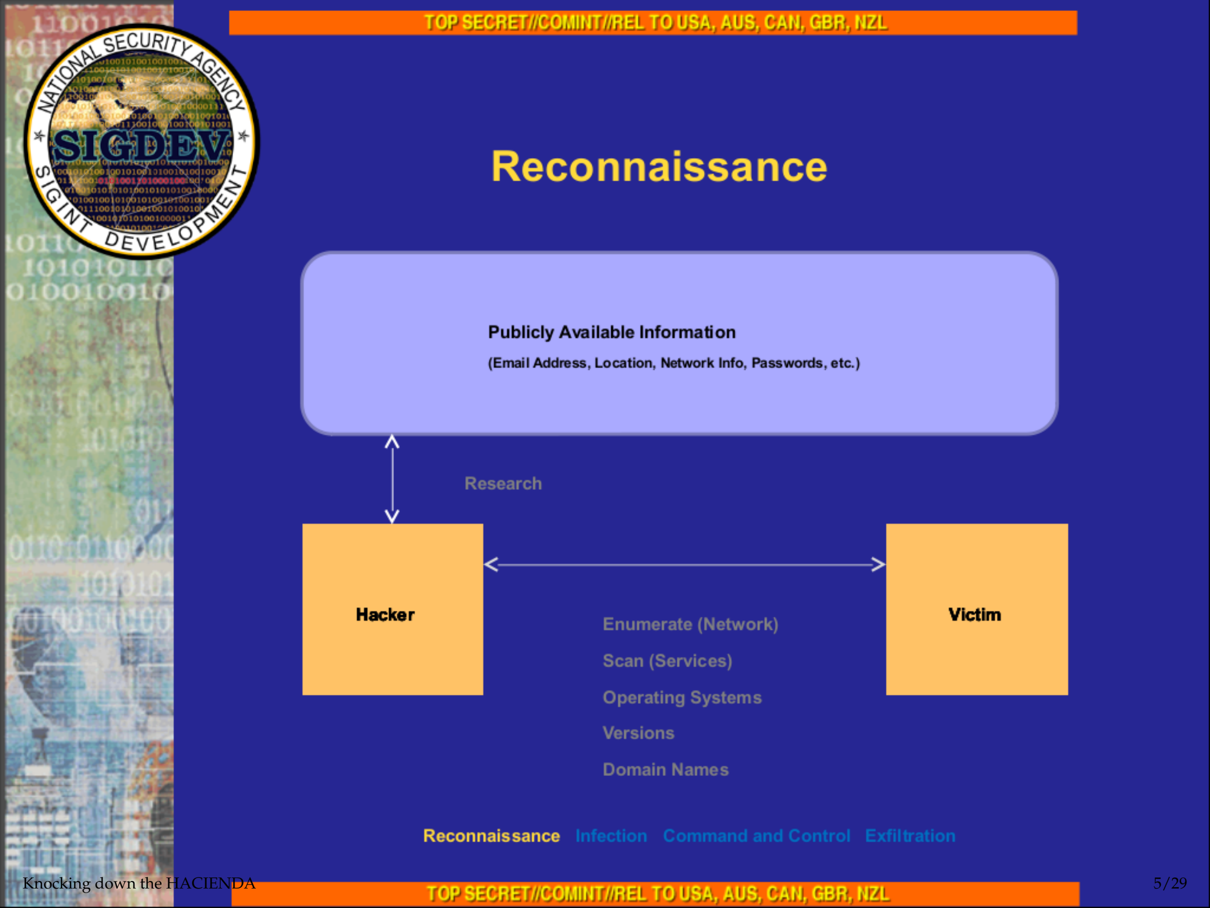
Step 3

Hacking in SIGINT



The Hacking Process

1. (**R**)econnaissance
2. (**I**)nfection
3. (**C**)ommand And Control
4. (**E**)xfiltration



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

Reconnaissance

Publicly Available Information

(Email Address, Location, Network Info, Passwords, etc.)

Research

Hacker

Victim

Enumerate (Network)

Scan (Services)

Operating Systems

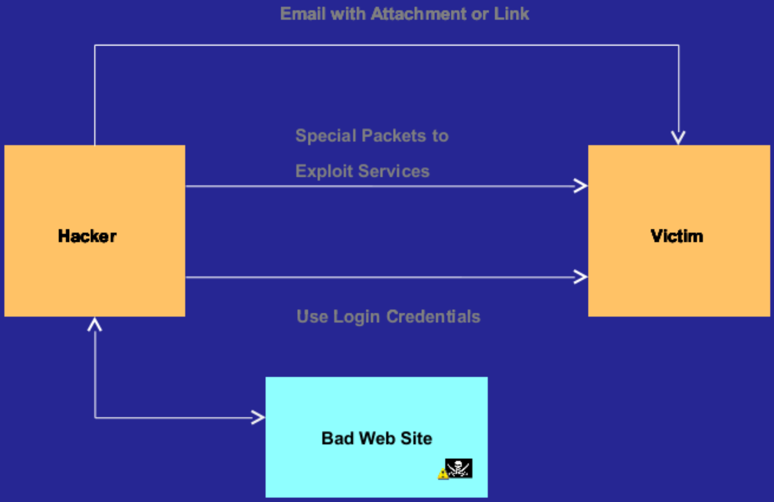
Versions

Domain Names

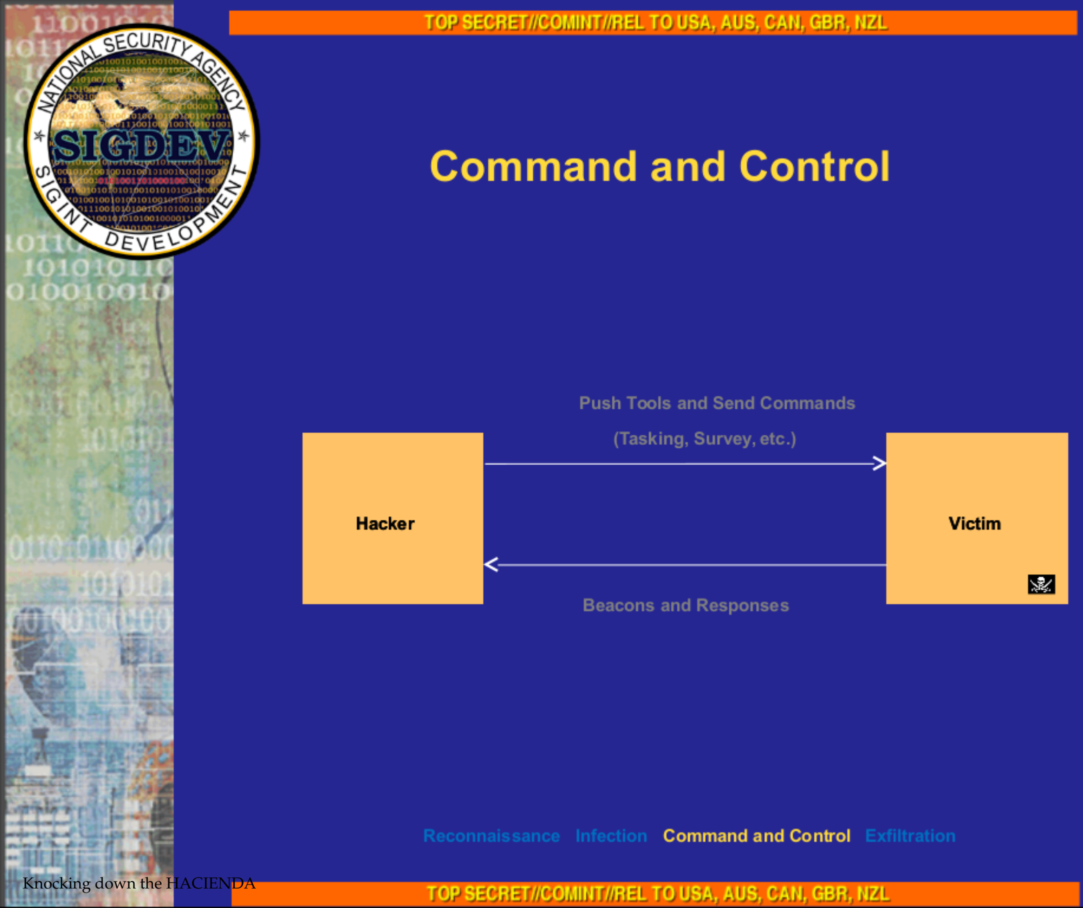
Reconnaissance Infection Command and Control Exfiltration

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

Infection



Reconnaissance **Infection** Command and Control Exfiltration



Command and Control

Push Tools and Send Commands

(Tasking, Survey, etc.)

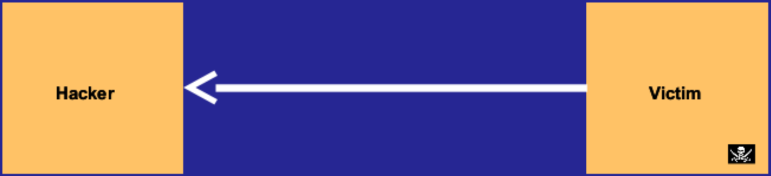
Beacons and Responses

Reconnaissance Infection Command and Control Exfiltration

Exfiltration

Exfil using known and custom protocols

(Known: HTTP, SMTP, ICMP, FTP, etc)



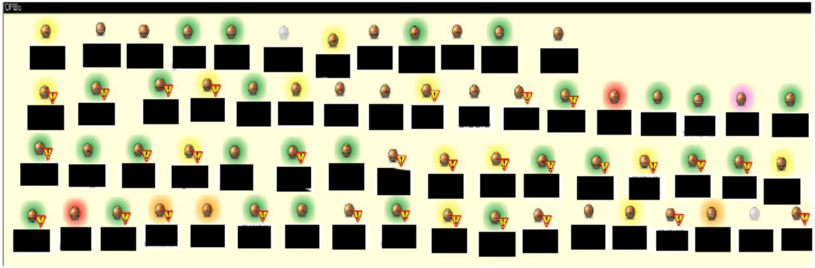
Reconnaissance Infection Command and Control Exfiltration

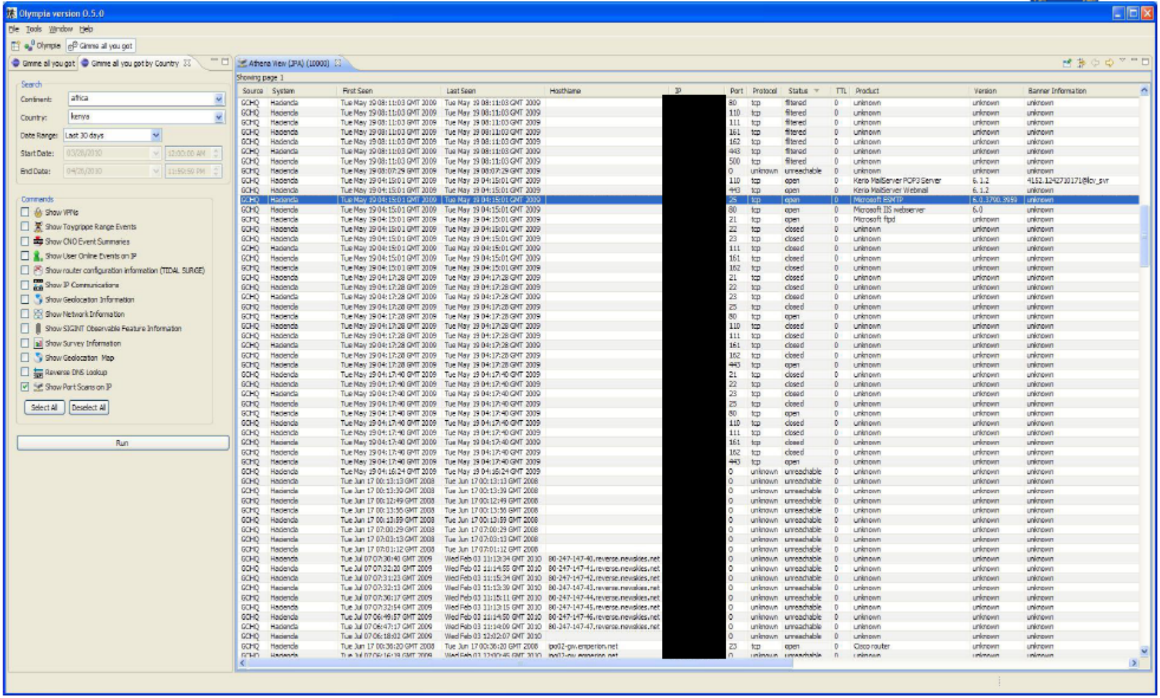
How is it used?

- CNE
  - ORB Detection
  - Vulnerability Assessments
- SD
  - Network Analysis
  - Target Discovery

LANDMARK

- CSEC's Operational Relay Box (ORB) covert infrastructure used to provide an additional level of non-attribution; subsequently used for exploits and exfiltration
- 2-3 times/year, 1 day focused effort to acquire as many new ORBs as possible in as many non 5-Eyes countries as possible





Search

Continent: africa

Country: kenya

Date Range: Last 30 days

Start Date: 03/28/2010 12:00:00 AM

End Date: 04/26/2010 11:59:59 PM

Commands

☐ Show VPNs
☐ Show Toygrippe Range Events
☐ Show CND Event Summaries
☐ Show User Online Events on IP
☐ Show router configuration information (TIDAL SURGE)
☐ Show IP Communications
☐ Show Geolocation Information
☐ Show Network Information
☐ Show SIGINT Observable Feature Information
☐ Show Survey Information
☐ Show Geolocation Map
☐ Reverse DNS Lookup
☑ Show Port Scans on IP

Select All | Deselect All

Source	System	First Seen	Last Seen	HostName	IP	Port	Protocol	Status	TTL	Product	Version	Banner Information
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	80	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	110	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	111	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	161	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	162	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	443	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:11:03 GMT 2009	Tue May 19 08:11:03 GMT 2009		[redacted]	500	tcp	filtered	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 08:07:29 GMT 2009	Tue May 19 08:07:29 GMT 2009		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	110	tcp	open	0	Kerio MailServer POP3 Server	6. 1.2	4152.1242710171@lcv_svr
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	443	tcp	open	0	Kerio MailServer Webmail	6. 1.2	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	25	tcp	open	0	Microsoft ESMTP	6.0.3790.3959	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	80	tcp	open	0	Microsoft IIS webserver	6.0	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	21	tcp	open	0	Microsoft ftpd	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	22	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	23	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	111	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	161	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:15:01 GMT 2009	Tue May 19 04:15:01 GMT 2009		[redacted]	162	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	21	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	22	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	23	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	25	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	80	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	110	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	111	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	161	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	162	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:28 GMT 2009	Tue May 19 04:17:28 GMT 2009		[redacted]	443	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	21	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	22	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	23	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	25	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	80	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	110	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	111	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	161	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	162	tcp	closed	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:17:40 GMT 2009	Tue May 19 04:17:40 GMT 2009		[redacted]	443	tcp	open	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue May 19 04:16:24 GMT 2009	Tue May 19 04:16:24 GMT 2009		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:13 GMT 2008	Tue Jun 17 00:13:13 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:39 GMT 2008	Tue Jun 17 00:13:39 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:12:49 GMT 2008	Tue Jun 17 00:12:49 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:56 GMT 2008	Tue Jun 17 00:13:56 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:13:59 GMT 2008	Tue Jun 17 00:13:59 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 07:00:29 GMT 2008	Tue Jun 17 07:00:29 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 07:03:13 GMT 2008	Tue Jun 17 07:03:13 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 07:01:12 GMT 2008	Tue Jun 17 07:01:12 GMT 2008		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:30:40 GMT 2009	Wed Feb 03 11:13:34 GMT 2010	80-247-147-40.reverse.nevskies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:32:20 GMT 2009	Wed Feb 03 11:14:55 GMT 2010	80-247-147-41.reverse.nevskies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:31:23 GMT 2009	Wed Feb 03 11:15:34 GMT 2010	80-247-147-42.reverse.nevskies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:32:13 GMT 2009	Wed Feb 03 11:13:39 GMT 2010	80-247-147-43.reverse.nevskies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:30:17 GMT 2009	Wed Feb 03 11:15:11 GMT 2010	80-247-147-44.reverse.nevskies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 07:32:54 GMT 2009	Wed Feb 03 11:13:15 GMT 2010	80-247-147-45.reverse.nevskies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:49:57 GMT 2009	Wed Feb 03 11:14:50 GMT 2010	80-247-147-46.reverse.nevskies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:47:17 GMT 2009	Wed Feb 03 11:14:09 GMT 2010	80-247-147-47.reverse.nevskies.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:18:02 GMT 2009	Wed Feb 03 12:02:07 GMT 2010		[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown
GCHQ	Hacienda	Tue Jun 17 00:36:20 GMT 2008	Tue Jun 17 00:36:20 GMT 2008	ipo02-gw.emperion.net	[redacted]	23	tcp	open	0	Cisco router	unknown	unknown
GCHQ	Hacienda	Tue Jul 07 06:16:19 GMT 2009	Wed Feb 03 12:00:45 GMT 2010	ipo02-gw.emperion.net	[redacted]	0	unknown	unreachable	0	unknown	unknown	unknown

- BUT, network analysis still manual!

[redacted]

- [redacted] GSM provider
- NSA TAO requested assistance gaining access to the network
- Network analysis using OLYMPIA:
  - DNS query to determine IP address
  - IP address to network range
  - Network range to port scan
  - Are there any vulnerable devices in that range?
- Duration: < 5 minutes

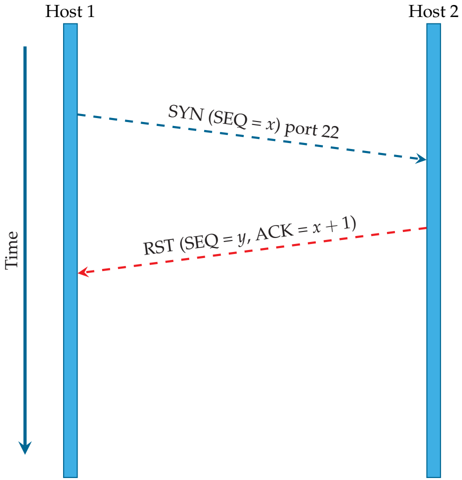
So, is it all lost?

Two Solutions

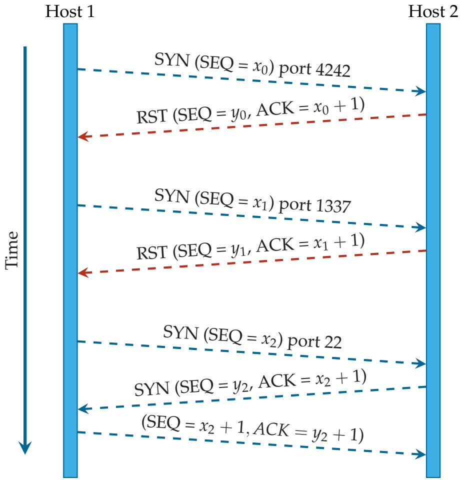
- Backwards-compatible minimally invasive hotfix (TCP Stealth)
- Clean-slate principled rearchitecture

An Introduction to Port Knocking

No knock, no fun

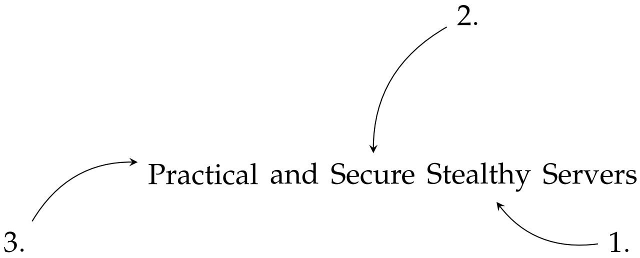


Port knocking example


Host 1
Host 2
Time
SYN (SEQ = x_0) port 4242
RST (SEQ = y_0, ACK = $x_0 + 1$)
SYN (SEQ = x_1) port 1337
RST (SEQ = y_1, ACK = $x_1 + 1$)
SYN (SEQ = x_2) port 22
SYN (SEQ = y_2, ACK = $x_2 + 1$)
(SEQ = $x_2 + 1$, ACK = $y_2 + 1$)

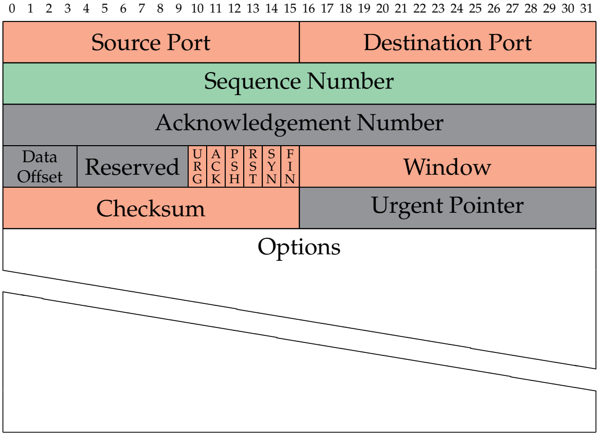
Design

Overview



Design

Stealthiness



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Source Port | Destination Port

Sequence Number

Acknowledgement Number

Data Offset | Reserved | URG | ACK | PSH | RST | SYN | FIN | Window

Checksum | Urgent Pointer

Options

Design (v1)

Security

- Destination IP address IP_d
- Destination port P_d
- TCP timestamp T

- Pre-Shared Key S
- Hash function h

Authentication Security Token (AV)

$$\text{AV} := h((IP_d, P_d, T), S)$$

- ISN := AV

SECONDDATE

- SECONDDATE is an exploitation technique that takes advantage of web-based protocols and man-in-the-middle (MitM) positioning.
- SECONDDATE influences real-time communications between client and server and can quietly redirect web-browsers to FA servers for individual client exploitation.
- This allows mass exploitation potential for clients passing through network choke points, but is configurable to provide surgical target selection as well.

Design (v2)

Security

- Destination IP address IP_d
- Destination port P_d
- TCP timestamp T

- Pre-Shared Key S
- Hash functions h, h'
- Payload p

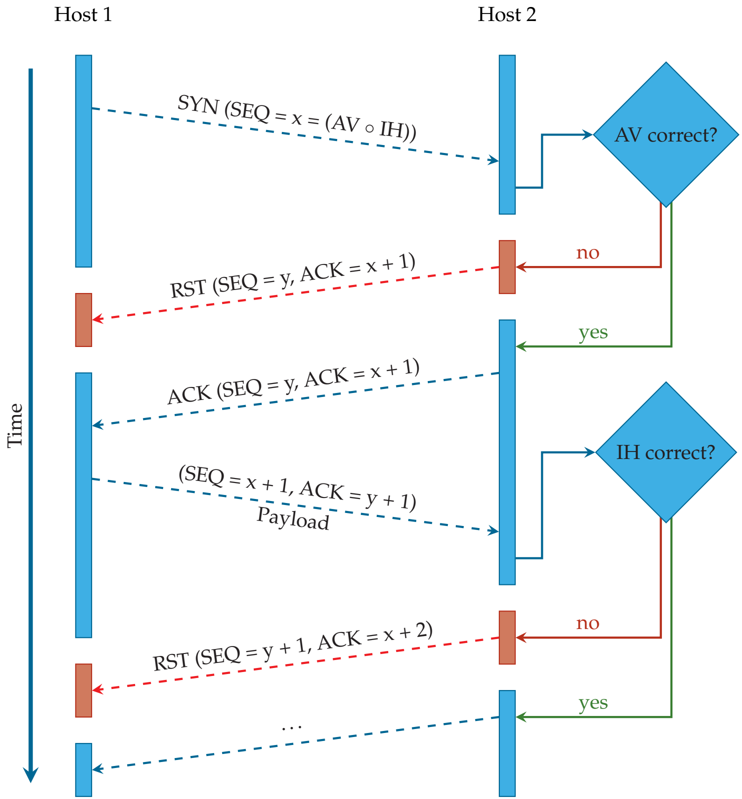
TCP Payload Integrity Protector IH

$\mathrm{IH} := h'(S \circ p)$

Authentication Security Token AV

$\mathrm{AV} := h((IP_d, P_d, T, \mathrm{IH}), S)$

- $\mathrm{ISN} := \mathrm{AV} \circ \mathrm{IH}$


Host 1
Host 2
Time
SYN (SEQ = x = (AV ∘ IH))
AV correct?
no
RST (SEQ = y, ACK = x + 1)
yes
ACK (SEQ = y, ACK = x + 1)
IH correct?
(SEQ = x + 1, ACK = y + 1)
Payload
no
RST (SEQ = y + 1, ACK = x + 2)
yes
. . .

Design

Ease of Use

- Source IP and Port *not* included in ISN generation
  ⇒ Compatibility with NATs
- Knocking is implemented *in the kernel*
  ⇒ No fiddling with config-files, firewall rules or daemons
  ⇒ Trivial to use from an application developer's perspective

Design

Ease of Use – TCP Stealth Server

```
char secret[64] = "This is my magic ID.";
int payload_len = 4;
int sock;

sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
if (sock < 0) {
        printf("socket() failed, %s\n", strerror(errno));
        return 1;
}
if (setsockopt(sock, IPPROTO_TCP, TCP_STEALTH, secret, sizeof(secret))) {
        printf("setsockopt() failed, %s\n", strerror(errno));
        return 1;
}
if (setsockopt(sock, IPPROTO_TCP, TCP_STEALTH_INTEGRITY_LEN,
               &payload_len, sizeof(payload_len))) {
        printf("setsockopt() failed, %s\n", strerror(errno));
        return 1;
}
/* Continue with bind(), listen(), accept(), recv(), ... */
```

Design

Ease of Use – TCP Stealth Client

```c
char secret[64] = "This is my magic ID.";
char payload[4] = "1234";
int sock;

sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
if (sock < 0) {
        printf("socket() failed, %s\n", strerror(errno));
        return 1;
}
if (setsockopt(sock, IPPROTO_TCP, TCP_STEALTH, secret, sizeof(secret))) {
        printf("setsockopt() failed, %s\n", strerror(errno));
        return 1;
}
if (setsockopt(sock, IPPROTO_TCP, TCP_STEALTH_INTEGRITY,
                payload, sizeof(payload))) {
        printf("setsockopt() failed, %s\n", strerror(errno));
        return 1;
}
/* Continue with connect(), send(), ... */
```

Design

Ease of Use – libknockify

- Shared library for use at compile- or run-time
- Enables TCP Stealth functionality for legacy code

```
$ LD_PRELOAD=./libknockify.so ncat knock-server application-port
```

- Configuration options (such as the TCP Stealth secret) are given as environment variables or via a special file

Limitations

- Distribution of the Pre-Shared Key
- ISN has only 32 bits

Limitations

- Distribution of the Pre-Shared Key
- ISN has only 32 bits
- Changes to ISN and TSVal by middle boxes:

	TCP Port		
Behavior	34343	80	443
Unchanged	**126 (93%)**	116 (82%)	128 (90%)
Mod. outbound	5 (4%)	5 (4%)	6 (4%)
Mod. inbound	0 (0%)	1 (1%)	1 (1%)
Mod. both	4 (3%)	13 (9%)	7 (5%)
Proxy (probably mod. both)	0 (0%)	7 (5%)	0 (0%)
Total	135 (100%)	142 (100%)	142 (100%)

Numbers by Honda et al. “Is it Still Possible to Extend TCP?”

Limitations

- Distribution of the Pre-Shared Key
- ISN has only 32 bits
- Changes to ISN and TSVal by middle boxes:

	TCP Port		
Behavior	34343	80	443
Unchanged	**126 (93%)**	116 (82%)	128 (90%)
Mod. outbound	5 (4%)	5 (4%)	6 (4%)
Mod. inbound	0 (0%)	1 (1%)	1 (1%)
Mod. both	4 (3%)	13 (9%)	7 (5%)
Proxy (probably mod. both)	0 (0%)	7 (5%)	0 (0%)
Total	135 (100%)	142 (100%)	142 (100%)

Numbers by Honda et al. “Is it Still Possible to Extend TCP?”

Working Code...

- Implemented for 3+ Linux kernel versions
- Implemented for FreeBSD
- Holger Kenn (MSFT) said would be easy to do in W32-Kernel(s)
- Sample client and server programs
- Patches for OpenSSH, GNUnet, systemd
- libknockify(.so) LD_PRELOAD
- Master's thesis, presentations, website, article in 5 languages
- Tested in big-endian/little-endian platforms (incl. compatibility)
- Draft has test vectors, detailed protocol specification
- Based on 1 year of community feedback, authors clueless about what else to do. Except find the right WG. Spencer solved that.

Why standardize...

- Port scanning is a well-known vulnerability. We need to address it.
- Implementations need to be compatible.
- Kernels must offer it for ease of deployment.
- Kernels will only ship by default if standardized.
- (Some GNU/Linux distributions already ship this anyway.)
- This does not solve all issues, but as many as we can with maximum backwards compatiability.

... and rough consensus?

Find more information at:

- `https://gnunet.org/`
- `https://gnunet.org/knock`
- `https://gnunet.org/gns`
- `https://gnunet.org/mcb`

Thanks to:
Julian Kirsch
Jacob Appelbaum
Monika Ermert
Laura Poitras
Henrik Moltke
Maurice Leclaire
Andreas Enge
Bart Polot
Luca Saiu
The Source

This work was funded by the Deutsche Forschungsgemeinschaft (DFG) under ENP GR 3688/1-1.

Slides will be at `http://grothoff.org/christian/`.