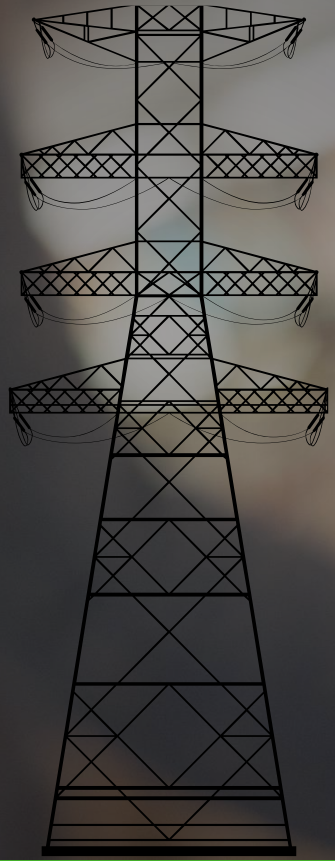
Automatic Discovery of Evasion Vulnerabilities Using Targeted Protocol Fuzzing

antti.levomaki@forcepoint.com
opi@forcepoint.com

FORCEPOINT
POWERED BY Raytheon
Protecting the human point.

black hat
EUROPE 2017

WHO?



ANTTI LEVOMÄKI

Research Scientist

OLLI-PEKKA NIEMI

Director of Research

WHAT?

NETWORK EVASIONS

+

FUZZING

=

Automated method for finding evasion vulnerabilities in modern up-to-date IPS & NGFW System

WHY?

- Evasions discovered by Ptacek and Newsham still work against modern IPS and NGFW system
- Lack of modern tools to highlight the risks of evasion vulnerabilities
- Configuring IPS systems to detect and prevent evasions can be really hard
- Increase the awareness to persuade vendors to fix evasion gaps

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

   mDyMX9-M989FP-aUPGV5-QGVXFV-xuFJpF-q5S3SM-bKE58w-CZ2Tv2-9wkLhu-s328g5

If you already purchased your key, please enter it below.
Key: _

NETWORK EVASIONS

- Result of a different interpretation of traffic by a security device than by the victim endpoint
- Robustness principle: "*Be conservative in what you do, be liberal in what you accept from others*", Jon Postel
- Ptacek & Newsham paper: "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection", 1998

INTRODUCTION TO EVADER

Applies evasion to attacks to bypass virtual patching and intrusion prevention.

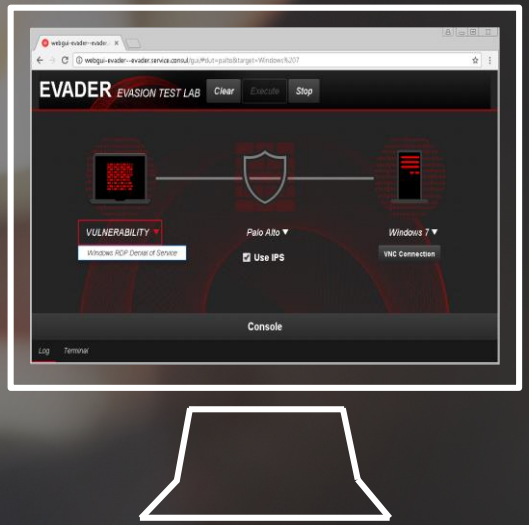
2009
Research published

2010
AET Threat Identified

2012
Evader released as freeware

2013
BlackHat Talk

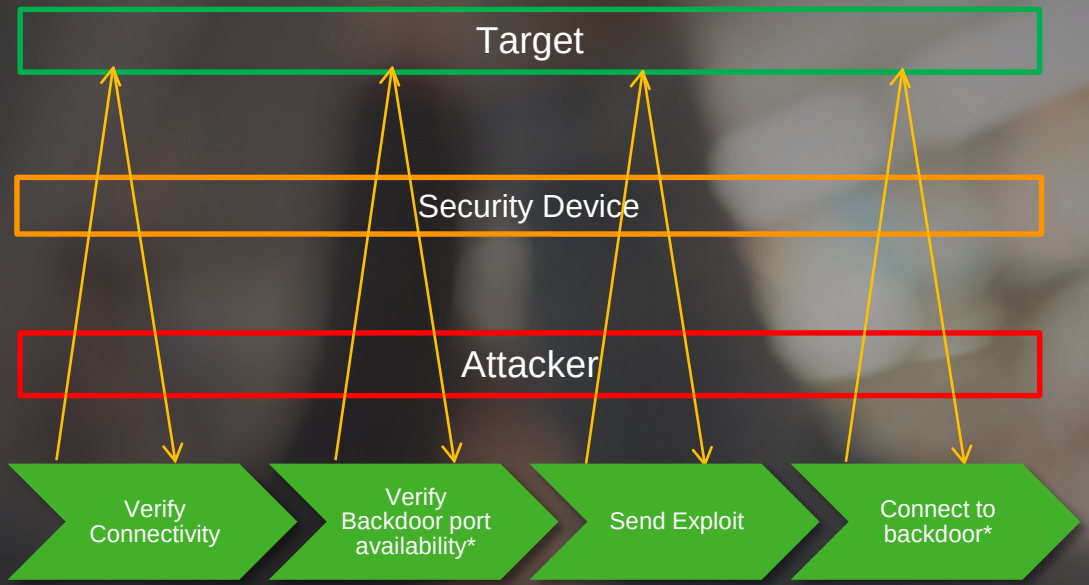
2017
Relaunch. AET Threat still present



EVADER

- Implements a few well known and old exploits to test traffic inspection
- Userspace TCP/IP stack with atomic evasions on all network layers
- Atomic evasions produce mostly valid transformations to traffic
- Combinations produce interesting traffic
  => at least 2^{45} - 2^{186} possible combinations depending on protocols
  => far too many to handle as a special case in IPS/NGFW

TEST METHODOLOGY



CVE-2008-4250, MSRPC Server Service Vulnerability

CVE-2004-1315, HTTP phpBB highlight

CVE-2014-0160 Heartbleed

*Heartbleed success is determined based on data leaked. No backdoor / post compromise

IDEA

- Cannot test all dynamic combinations
  => generate random combinations and test them rapidly

- Cannot ensure that all combinations produce valid traffic
  => use real exploit and victim host. If the exploit works, traffic is valid.

- Cannot know what the IPS/NGFW is doing
  => configure to terminate everything it thinks is malicious.

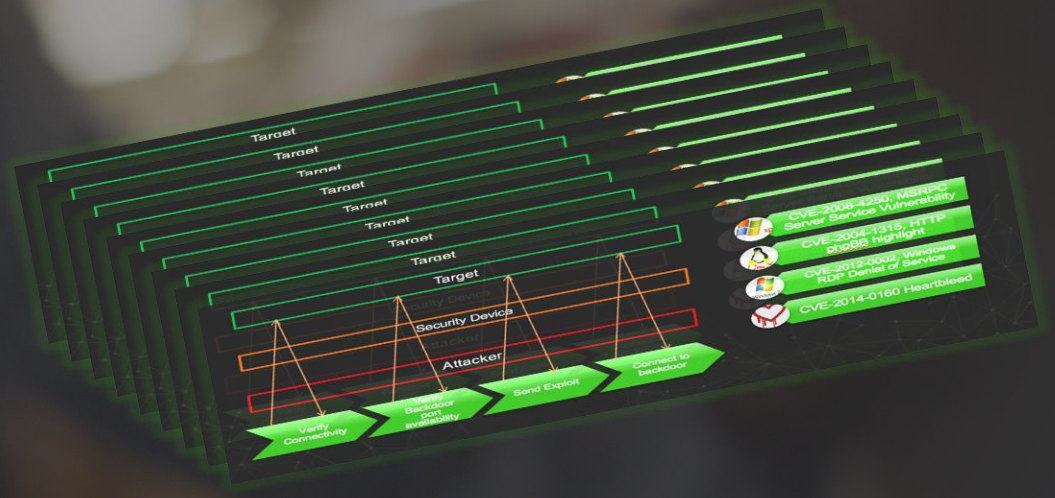
MONGBAT

- Fuzz generator for Evader, runs parallel Evader instances with random evasion combinations targeting specific parts of networking protocols.
- Handles addressing and validates the test environment.
- The evasions and their parameters
  are selected from the set Evader lists as supported.
  => validation scripts to drop completely useless combinations
  => each run is different

MONGBAT

Successful attacks are recorded for repeatability

- Evader command line including
  - Evasions and parameters
  - Random seed
- Packet captures




DEMO

RESULTS

Success/attempts in 10 minutes of fuzz testing

Vendor	HTTP	HTTPS	Conficker	Heartbleed
Vendor I	72 / 12364	crash[a]	21 / 858	0 / 557
Vendor II	133 / 8481	97 / 4119	16 / 2368	25 / 899
Vendor III	126 / 8788	277 / 4059	15 / 1204	40 / 1092
Vendor IV	746 / 1833	N/A[b]	2 / 1077	N/A[b]
Vendor V	3366 / 8975	2550 / 5970	8 / 3561	50 / 891
Vendor VI	0 / 7366	0 / 6337	0 / 7778	0 / 994

RESULTS

Low level evasions can be payload independent

=> TCP layer evasion discovered with HTTP attack likely also works with HTTPS & SMB/MSRPC

Vendor	HTTP	HTTPS	Conficker	Heartbleed
Vendor I	H			
Vendor II	P, C	T, H	P	T
Vendor III	P, H	P, C, T, H	P	P, C, T
Vendor IV	P, C, H	P, C, T, H	C	P, C, T
Vendor V	P, C, T, H	P, C, H		T
Vendor VI				

P = PAWS
C = TCP_CHAFF
H = HTTP
T = TLS record layer segmentation

CHALLENGES – VENDORS ARE BLOCKING THE TOOL

WHAT	Block the tool	FIX
DE:AD:BE:EF	Prevent testing by blocking MAC	Changed MAC
User-Agent “Railforge”	Block attack based on User-Agent	Change User-Agent
TCP Syn Windows Scale 0	Prevent testing by blocking SYN packets	OS Spoof to mimic Windows, Linux during 3-W HS
Identify Shellbanner	Block post compromise and prevent success validation	Different mechanism for success validation or custom shell banner
High port blocking	Block post compromise and prevent success validation	Inline shell, visual effect or ack based success indication
Blacklist	Blacklist IP or subnet used for testing	Legitimate clean test pre-exploit test validation

KEY FINDINGS

1. Rapid discovery of working evasions
2. Very difficult to tune security policies to be evasion-proof
3. Low level (TCP) evasions can be payload independent
4. One (1) reliably working evasion is enough to bypass security completely.

For questions and access to EVADER contact Olli-Pekka Niemi opi@forcepoint.com

antti.levomaki@forcepoint.com

opi@forcepoint.com

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.