

Matt Graeber Subverting & restoring trust in Windows

get authenticode signature in
PowerShell against MS binary
(legit binary will pass) if compared
against known good binary

sigcheck from SysInternals

a signing cert is only as good as
the security of the private key

modify 2 registry keys to beat
this! You can become Microsoft

Sign your code w/ PowerShell

context is everything in security
research

github.com/mattifestation
github.com/PowerShellMafia

Never trust an unknown system
compare against known good system

use multiple points/checks to establish
~~the~~ trust

what does trust actually mean?

document your failures & keep your
old stuff

Mr. Stewart

Subject: 4-12-1981

not authentic signature in
letter shell against the binary
(right binary will pass if compared
against known good binary)

check from system

a binary set is only as good as
the security of the private key

modify 2 registry keys to test
this! You can remove Microsoft

sign your code in Powershell!

content is everything in security
context

difficult to find a solution
in Powershell

never trust an unknown system
compare against known good system

was multiple possibilities to establish
the trust

when does trust actually mean?

different way to trust a binary
old style

John Strand

Hacking, AI, Bullies, Pie, Mom and Cancer

Competitive analysis clauses in license agreements prevent free exchange of some research (e.g. "release your exploit & we'll sue")

Public interest may stop this (i.e. say your acting in public interest)

~~Consumer Fairness~~

Consumer Review Fairness Act

Be willing to try new things

Don't give up... even in the face of massive data breaches

Talk to people who are employed at breached firms

Malware beaconing: regular intervals, data size, connection time

~~git~~ github.com/ocmdev/rita

Give till it hurts... and invite your friends

We have the power to be awesome or incredibly evil. Choose awesome!

John - 1991

Hacking, AT Bellini, Pie, Mum and Carol

Investigative analysis classes in library
university prevent free exchange
of some knowledge "information
exploit & well away"

Public interest may stop this (ie
any form of public interest)

~~Consumer Fairness Act~~
Consumer Fairness Act

Be willing to try new things

Don't give up when in the face
of massive data breaches

Talk to people who are employed at
various firms

Multiple businesses: regular intervals
info size, conversation time

get a little bit of info/contacts/into

bring till it meets... and invite your
contacts

We have the power to be successful
or miserably fail. Success and failure

Bruce Potter

What to test and how to test it

More to life than pen-tests

We can learn from existing software testing techniques

Why to test? errors in security functionality, errors that lead to security weaknesses, errors in architecture design, errors in implementation

testing is integral to secure development & operation

it's more cost effective to do gray box or white box testing; at least partial knowledge of system

~~Systems generally need~~

Why do you now care about security?

Who is your adversary?

What do you expect from testing process?

What is NOT tested? Note this too

Short term & long term remediation

All testing starts w/ risk

No testing has complete coverage:
test the stuff most likely to be
attacked

Do architecture & design review

Think conceptually about how to
break system

Beyond xp_cmdshell

github.com/netSPI/PowerUPSQL

SQL server has robust auditing
USE IT!!

xp_cmdshell is usually monitored... try
to avoid it

can use CLR assemblies to run
on SQL server

Download code from internet
via TSQL

github.com/EmpireProject

slideshare.net/nullbind

Beyond XP - endwell

github.com/Project

XP server has robust auditing
!!!

XP endwell is heavily monitored... try
to avoid it

can use CLR assemblies to run
on XP server

Downloaded code from internet
via TSP

github.com/Project
alibaba.com/Project

Deral Heiland

IoT security: Executing an effective security testing process

embedded hardware
mobile & control apps
cloud & APIs
network communication
data

functional eval: deployed it normally
& look at it (1 running normally & 1
target... compare the two)
map out features & functions

recon, recon, recon...

go to FCC and look up the device
by FCC ID

Mobile & control
encryption (~~stored~~ storage & transmission)
authentication
access rights
communication protocols
SSL pinning

cloud & web APIs
encryption (storage & transmission)
auth & session management
common web vulns
XSS, CSRF, SQLi, etc

Network
exposed services
auth
access rights

Physical embedded hardware inspection
chips
~~ph~~ physical ports
circuitry connection

Radio (RF)
encryption
pairing
access control
replay attacks

This all leads to reduced issues,
reduced risk, better products, &
deeper understanding

Purpose driven hunt

hunting is actively searching for malicious activity in environment

assume breach mindset

generic process: gather data & hunt for "bad"

what is "good"? what's normal in your ~~env~~ network?

create hypothesis (what are you seeking?)
gather data
hunt for bad

how to make a hypothesis?

assume breach

focus on post exploitation activity

MITRE cyber attack lifecycle

focus on ~~the~~ behaviors, rather than attacker's tools

- ① identify the tactic & technique
- ② identify the procedures
- ③ identify collection requirements
- ④ identify the scope
time
data to collect
- ⑤ document excluded factors

this lets you focus on a tangible result

don't stop the tool, stop the techniques it uses

don't bite off more than you can chew

no "golden bullet"

iterative process

don't settle for 1 detection technique

How the equation groups 2013 tools
pwn in 2017

April 2017: shadow brokers tool drop

most of it was post-exploit

around 2005: Danderspritz framework

Fuzzbunch (kinda like Metasploit Framework)

PeddleCheap (implant, part of command & control)

Danderspritz written in Java
plugins written in Python
designed for stealth

survey.py script (what's running on target... everything!)

Danderspritz has forensics capabilities

has extensive database of anti-malware systems; via registry queries, it spots things

safety handlers: keep users from getting caught by stopping them from doing actions that would get them caught

EmptyKey for WMI abuse

danderspritz.com

danderspritz_docs github

Anti-phishing & malware measures

rootisthelimit.com

~~kill chain~~
~~pre~~
~~email~~

domain typo squatting \Rightarrow Python
derbycon1.com DNS twist
derby-con.com on github.com

block attachments & review those
you let through

Use Outlook add-ins such as
PhishAlert, PhishReporter, or PhishMe

Windows tags stuff coming from
internet via Alternative Data Streams

software restriction policy... via
Active Directory group policy
%TEMP%\ } block anything
C:\Windows\Temp\ } running from
here

subtee's app whitelist bypass
subt0x10.blogspot.com

block parked domains

block webmail access

mas. timilertteyogor

10/10/2020

\Rightarrow $\text{Pythos} \Rightarrow \text{Pythos} \text{ type something}$
 $\text{Pythos} \Rightarrow \text{Pythos} \text{ type something}$
 $\text{Pythos} \Rightarrow \text{Pythos} \text{ type something}$

2: Windows / Temp /

www.dreamtore.com

black backed shrike

2022, January 20

Tyler Hudak

To catch a spy

Got to have logging, visibility into your systems to spot these techniques

Most importantly, need knowledge to find this stuff!

Image file execution options
attach a debugger to a program
prior to run... registry key

sticky keys backdoor... registry key

Detection: look for use of debugger
registry keys (MS Autoruns)

Can also detect via logging

Shell extensions
very tricky to find

DLL search order
checks first in program dir, then
|windows\system32, then |windows|
system, |windows, current dir,
and lastly in path

malware wants to get in closest
to the front

malware often tries to use
fxsst.dll

Detecting this is easiest w/ memory
dumper utils like Volatility

Volume boot record persistence
reimage... make sure master boot
record is overwritten!

Detection via memory analysis

Process hollowing
again, memory analysis to detect
sysmon w/ parent process analysis

Casey Rosini

Memory-based library loading

Has been around for awhile, but
a little ~~obscure~~ obscure

portable executable (PE) format
exe & dll are similar

DLL: module w/ things for another module

~~ex~~ DLL entry point is optional

Casey Rosini

Memory-based library loading

has been around for awhile, but
a little obscure

portable executable (PE) format
exe & dll are similar

DLL: module w/ things for another module

~~and~~ DLL entry point is optional

Blue team keeping tempo w/offense

the stronger your competitor, the stronger your game

low-level visibility at the endpoint is pervasive

how to sift huge amounts of endpoint data?!?

detection & prevention have improved
app control, endpoint & network flow

good techniques will be commoditized & eventually won't work; signatures will be developed

get the right tools & data

atomic testing: small unit tests
based on MITRE ATTACK framework

don't fixate on alerts... what was the attack behind it? What technique was used in the attack?

watching memory is fine, but eventually, a network packet will be sent by an attack (knowingly or unknowingly)
i.e., network connection by Windows command line

an attacker might get in, but he must
fight to get something out

Data mining wireless surveys

~~ELK stack~~ (Elastic search, ^{Logstash} ~~Logstash~~, Kibana)

scapy doesn't parse PPI header
(for GPS coordinates)... tshark does

Logstash for log processing

most packets were from channels
1, 6, 11

top SSIDs: xfinitywifi, xfinity,
sle, cablewifi, coxwifi

ELK stack
Elastic search
Logstash
Kibana

Alfa cards draw a LOT of power
from USB

~~Ryn~~ A

Ryn gold Alfa card on USB 3 port,
due to higher data thru put on
5 GHz band

Data Mining wireless surveys

ELK stack (Elastic search, Logstash, Kibana)

Logstash doesn't parse PPT headers
(for GPS coordinates) in network logs

Logstash for log processing

most packets were from channels
11, 12, 13

top fields: xfinitywifi, xfinity
etc, cmlb, viti, cox, viti

ELK stack
Elastic search
Logstash
Kibana

Afterwards I had a lot of trouble
from USB

Run on A70 with USB 2 port,
due to network data that got on
2 USB ports

TIM TOMES

Burping for joy & financial gain

use grep extract... it's cool & works well (especially on HTTP response)

method interchange

right click w/in repeater to switch get & post (and vice versa)

test for SSL/TLS stripping
proxy, request handling, force use of SSL

can strip HSTS, but only if man-in-the-middle is there for first HTTPS request

TIM TOMES

Building for joy & financial gain

use deep extract, it's cool &
works well (especially on HTTP
responses)

method interchange

right click when reporter to switch
get & post (and vice versa)

test for self's stripping
proxy, request handling, force use of
SSL

can strip HSTS, but only if man-in-
the-middle is there for first HTTPS
request

Cheating to win w/web app security

identify what's important to test

~~all~~ arbitrary data can be sent;
assume that

have no control over client

OWASP top 10, but don't stop there
developers will use 3rd party components

frequent web app testing

decide on black, white, gray box
testing... maybe a combo of these

internal tests should be white
or gray box

recon, map, discovery, exploit

focus with purpose (if you're
stuck, move on & come back to it)

Aggressive backups & patch faster;
if patch fails, roll back

checking to see if we can
exploit

test of whether it's important to test

that arbitrary data can be sent
assuming that

there's no control over client

WMAF top 10, but don't stop there

developers will use 3rd party components

different way of testing

decide on black, white, gray box
testing... making a combo of these

internal tests should be white

OT gray box
black box, recovery, exploit

tools with purpose (if you're
stuck, move on & come back to it)

Adversary package & tool (first)
if better tools will back

Full-contact recon.

packet economics; be judicious about sending packets to a target
each packet = chance of getting caught

the older a target, the more vulns it likely has

ptrarchive.com (reverse DNS back to 2008)

google's ~~cert~~ cert transparency report

sublist3r ~~is~~ tool

remember shodan!

githump tool (each github commit has an email attached to it)

data.com (finding soft targets)

hunter.io

verify-email.org

allmytweets.net

finder.insidepro.com (hash cracker)

Full-contact recon
each packet = 10000
packet economics: be judicious
about sending packets to a target

the other a target, the more likely
it likely has

gathering.com (reverse DNS back
to 2000)

people's or cost transparency report

publicist 37 tool

remember should!

gathering tool (each group commit has
an email attached to it)

data.com (finding soft targets)

ai, target
verify-mail.org
any, security

finder.indeedpro.com (much cracker)

I want my EIP

stack buffer overflow on wikipedia

ESP register: top of stack

EIP register: next instruction to be executed (it's address)

we want to put a return address into EIP that we control. This leads to code execution, as we want to send EIP to our code

need to know how much input causes the buffer overflow

~~pattern~~ pattern_create.rb in MSF
this is so we can find exact input which caused EIP overwrite

pattern_offset.rb in MSF (tells exact position of the pattern we want)

we need a memory location containing JMP ESP, to go to EIP (that we control address of)

github.com/hardwaterhacker
hardwatersec.blogspot.com

I want my EIP

stack buffer overflow on wikipedia

EIP register: top of stack

EIP register: next instruction to be executed (its address)

we want to put a return address
into EIP that we control. This leads
to code execution as we want to
send EIP to our code.

need to know how much input causes
the buffer overflow

pattern offset to EIP in MEF
this is as we can find next
input which causes EIP overflow

pattern offset to EIP (tells exact
position of the pattern we want)

we need a memory location containing
JMP EIP, to go to EIP (that we
control address of)

disturb.com/waterhacker
msb.trapsol.blogspot.com

100 million secrets: recent password dumps

people often choose secrets as their passwords

hackermaps.org

password sources: data breaches
haveibeenpwned.com

hashes.org

review your wordlists against recent dumps

remove long strings, unicode from wordlists

leet speak passwords aren't used that much

iwant, ilove, ihate, ... very popular beginnings of passwords

season + year is popular "summer 2016"

github.com/nyxgeek/dumpsniffer

10 crack commandments at hashcrack.io

100 million accounts: recent password dumps

people often choose secrets as their passwords

passwords.org

password sources: data breaches
havepasswords.com

passwords.org

review your wordlists against recent dumps

remove long strings, unicode from wordlists

last year's password dumps don't need that much

beginnings of passwords
want, i love, i hate... very popular

passwords that are popular "summer 2016"

github.com/hackbook/dumpcrackmap

if crackmap is not working

Ryan Reid

~~by~~ SpyDir: a Burpsuite extension

github.com/aur3lius-dev

dyn. dynamic spidering & low on time

~~By~~ Burpsuite Pro content discovery

what if you have source?

Needs Jython 2.7

in BApp store (older version)

Ryan Reid

Topic: a purpose extension

github.com/forthepeople

the dynamic equilibrium of law on time

Part 9: Purpose for content discovery

what if you have sources?

Version 2.1

in BGP state (older version)

Sarah Norris

Phishing for you & your grandma

need pretext w/ urgency
good payload
evade spam filter
good phishing site

mxtoolbox

sourceforge.net/projects/opendkim
edit /etc/opendkim.conf
add DKIM key to DNS

setup SPF, DKIM, DMARC

get an ssl cert
letsencrypt

unicorn.py (post-exploit framework)

Pretext possibilities

open court case

relevant news

relevant events

something impacting target

Sarah Morris

Blindfold for you & your group

need to get up
good, good, good
good, good, good
good, good, good
good, good, good

next box

across for net/propaganda
edit text/propaganda
and DTM box to DMS

setup 25, DTM, DMS

get on 25, 25
1/25/25/25

university (post-explicit framework)

post-explicit
open court case
relevant news

relevant events
something important target

Lennart Koopmann

Love is in the air: DFIR and IDS for wifi networks

~~WTF. Horse~~ <https://wtf.horse>

wifi security is a mess, hard to secure & attacks aren't that hard

802.11 management frames: how client & access point connect

probe request: client device asking if a known network is in range

probe response: yes, I'm the known network you asked for

WPA-PSK is still sniffable, if you have the pre-shared key
must kick someone off & catch their ~~connect~~ initial connection
(ala aircrack-ng)

hard to analyze wifi packet captures over time in Wireshark/tshark

Nzyme github.com/lennartkoopmann

92-rod, 1/2" length, 2000/1000

the 11th and 12th centuries

known restaurant you ordered for
grocery responses yes, I'm the

WPA-Part is still ambiguous if you
have the pre-ambled key
what I've seen is off-kilter
their ~~ambiguity~~ initial conversation
(no other of-vo)

<https://github.com/leandropereira/algorithm>

Matthew Eidenberg

SniffAir open source wireless security assessment framework

look at beacon frames: they contain
MAC, SSID, encryption type, etc

look at probe requests & probe responses

sniffair designed to analyze &
manage large amounts of data

~~modular~~ modular & supports several
attacks (EAP password bruteforcing, captive
portal fake, etc)

github.com/tylous/sniffair

Matthew Eidelberg

difficult to open source wireless security
management framework

look at beacon frames; they contain
MAC, SSID, encryption type, etc.

look at probe requests & probe responses

sniffair designed to analyze &
manage large amounts of data

sniffair modular & supports several
attacks (EAP password bruteforce, capturing
portal fcs, etc)

difficult to analyze/sniffair

Tim Malcolm Vetter

Privacy Game Tim Malcolm Vetter

separate identity from physical address

can you truly get privacy?

"How to be invisible" by JJ Luna

pay in cash

get a deed & title in LLC name
get an LLC thru trusted attorney
that understands privacy

can get a car via LLC

get a mailing address via UPS store
do this while driver license has
old address or your passport

home insurance policy can be a pain
but it's possible

most times, people don't need physical
address ("This is my address")

VPN traffic to disguise source IP

Tim Malcom letter

Privacy from Tim Malcom letter

separate identity from physical address

can you truly get privacy?

"How to be invisible" by JJ Luna

boy in code

get a hard drive in the house
get on the internet with a trusted attorney
that understands privacy

can get a car via the

get a mailing address via the store.
do the white driver license has
old address or your passport

how internet policy can be a pain
but it's possible

most times, people don't need physical
addresses ("this is my address")

VPN traffic to disguise source IP