

2019

ADVERSARY SIMULATION



- DATASHEET -



From cyber criminals who seek personal financial information and intellectual property to state-sponsored cyber attacks designed to steal data and compromise infrastructure, today's advanced persistent threats (APTs) can sidestep cyber security efforts and cause serious damage to your organization.

A skilled and determined cyber criminal can use multiple vectors and entry points to navigate around defenses, breach your network in minutes and evade detection for months.

APTs and cyber criminal organisations present a challenge for today's organizational cyber security efforts.

STATE OF PLAY

```
viernes 9 novembre 01:31:32 2018 ]-[ ~/Lamport ]
$ gcc lamport.c base64.c -o lamport -lcrypto

viernes 9 novembre 01:31:34 2018 ]-[ ~/Lamport ]
$ ./lamport -g
[+] Calculating Lamport keypair . . .
[+] Obtaining random data from a secure source
[+] Calculating the public key from the private one

-----BEGIN LAMPOR PRIVATE KEY BLOCK-----
Dnuw/2KD0ifxuigGdIJiJ9rfhkJaucOafAhsjB/YVfQVCNSi1EmKHL+9ZPt2I7e
USQbcc0cn++tFEs8kVRMlgCYHhFT5AdlV3eKo1ZmXT/lQcPfNv6tdYmjMtPgyOuP
W46wFWRV0hCjZzv6hNo0101nZldsceQXqQmcy8/gtg+cJB+mZ0GLk1pyu290BF15
RHdtcU8VlUhU3/9rPVya/iJltz9ec2XblARA90a8LQ012MhAfho8avPIAS1vah6p
K0HMrUV3hVgjyns5sy7ss2mevH35GF19XTZwHJ4hWycDsfgTb3K1n58PQZwWnDxy
s8RqgaEhbVdCPRPQQFNKVBI1G8SgVbhx0bgTDdFYlsPX0ro0hxGYcw49/W62w3ef
ZuFAxog3td15EF0gLL35RzpEaRH608GrS3oEqPfdg5wn7Z24rb9fx1R6q8n0H0/T
N18Nv3EYJ7XG6LJVPtCExvpC38fhkaLNB81gXVBNQR1ue6DwHCP5eC8gLNhucM3
RhdQ1RM2wEj1JPthq5bq7Y7v+h1w+66H2M1H0QDL87AdxLWTracW000sup486rwy
Hkqzs406XQvfruzHZ18gTEU1VwQ1w+PeKJKE7Cw4KFFvG2B8n08EcPy8C3H0M2
0ubZvQ6CZ4r8AeZQvQ62apfQ29wCVpe+421uTb7LS+4LX7J0Mf+17B8w03pne4Q2v

d the user to tell me what the fuck should I do
on)
e(argv[0]);

n & 1) // Signing the message

performing the "calculation" of the signature
i = j = 0; i < HASH_SIZE_BYTES; i++)
if(hash[i] & 0x80) // MS-bit of the byte 10000000b
memcpy(signature + j * HASH_SIZE_BYTES, private[i][1], HIGH_SIZE_BYTES);
else
memcpy(signature + j * HASH_SIZE_BYTES, private[i][0], HIGH_SIZE_BYTES);
j++;
if(hash[i] & 0x40) //
memcpy(signature + j * HIGH_SIZE_BYTES, private[i][1], HIGH_SIZE_BYTES);
else
memcpy(signature + j * HIGH_SIZE_BYTES, private[i][0], HIGH_SIZE_BYTES);
j++;
```

How We Can Help

Abditive Cyber Security can help your organisation in identifying weaknesses across your people, processes and technical controls.

We simulate real world attacks against your organisation by first profiling your digital footprint and planning our attacks accordingly following this initial phase. This is known as Open Source Intelligence Gathering (OSINT) .

Following this discovery phase, Abditive will deploy & develop infrastructure used to perform phishing and to allow for command and control communication out of your organisation.

Criminal and nation-state adversaries are moving towards alternative methods of egress, using Microsoft software such as OneDrive, Skype for Business, Office365 and Exchange to communicate with their implants.

Abditive is able to deploy similar custom implants, alongside traditional HTTPS/DNS implants, to attempt to evade and assess your security controls. Combined with rigorously QA'ed pre-phishing, bulk phishing and spear phishing campaigns, we can emulate real world attacks in a safe and controlled manner, updating you with wash up calls every step of the way.

Alongside assessing technical controls, we can perform physical social engineering assessments, using our third party Hungarian ex-special forces contractors.

Our Team

Abditive Cyber Security's technical centre of excellence operates in Budapest, Hungary.

Our testers are recruited from the top technical information security universities in the region. Holding internationally recognised certifications from SANS, Offensive Security and CREST - our consultants can provide security testing at an international standard.