RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MBS-T08

Mobile Security and the Post-Perimeter World:
10 Years of Mobile Threats

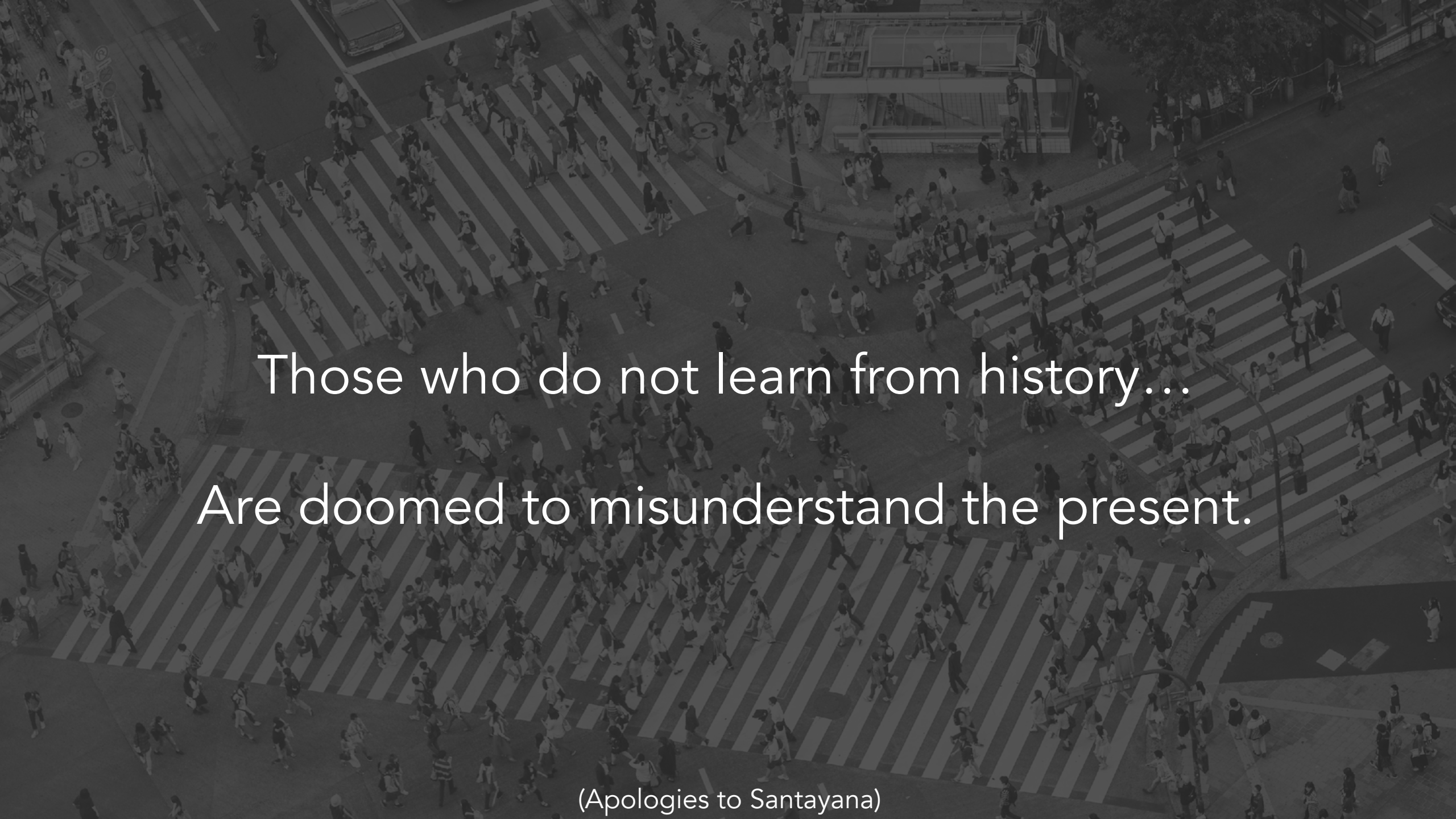
Apurva Kumar

Staff Security Intelligence Engineer, Lookout
apurva.kumar@lookout.com
Twitter: @abby_kcs

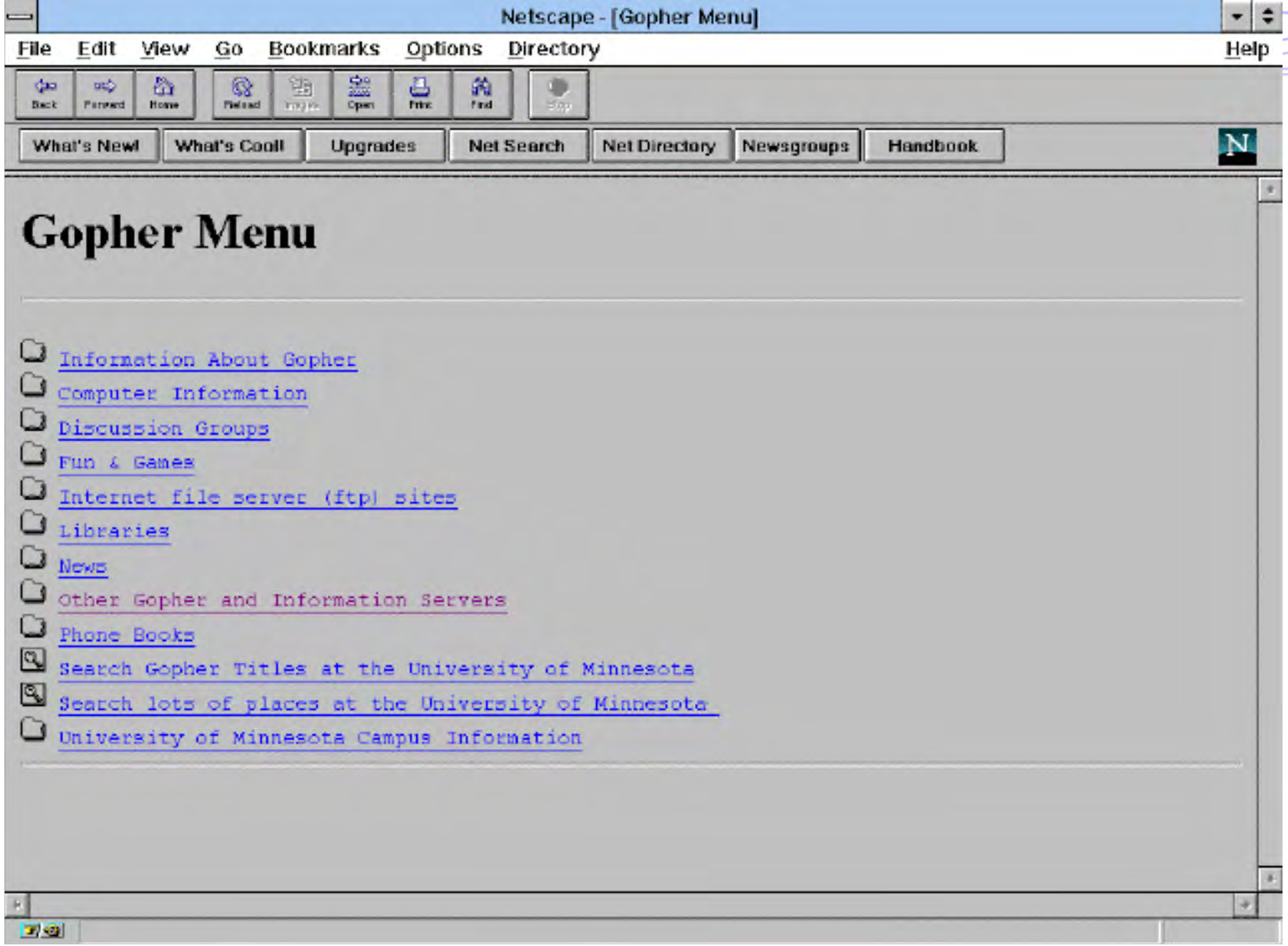
Michael Murray

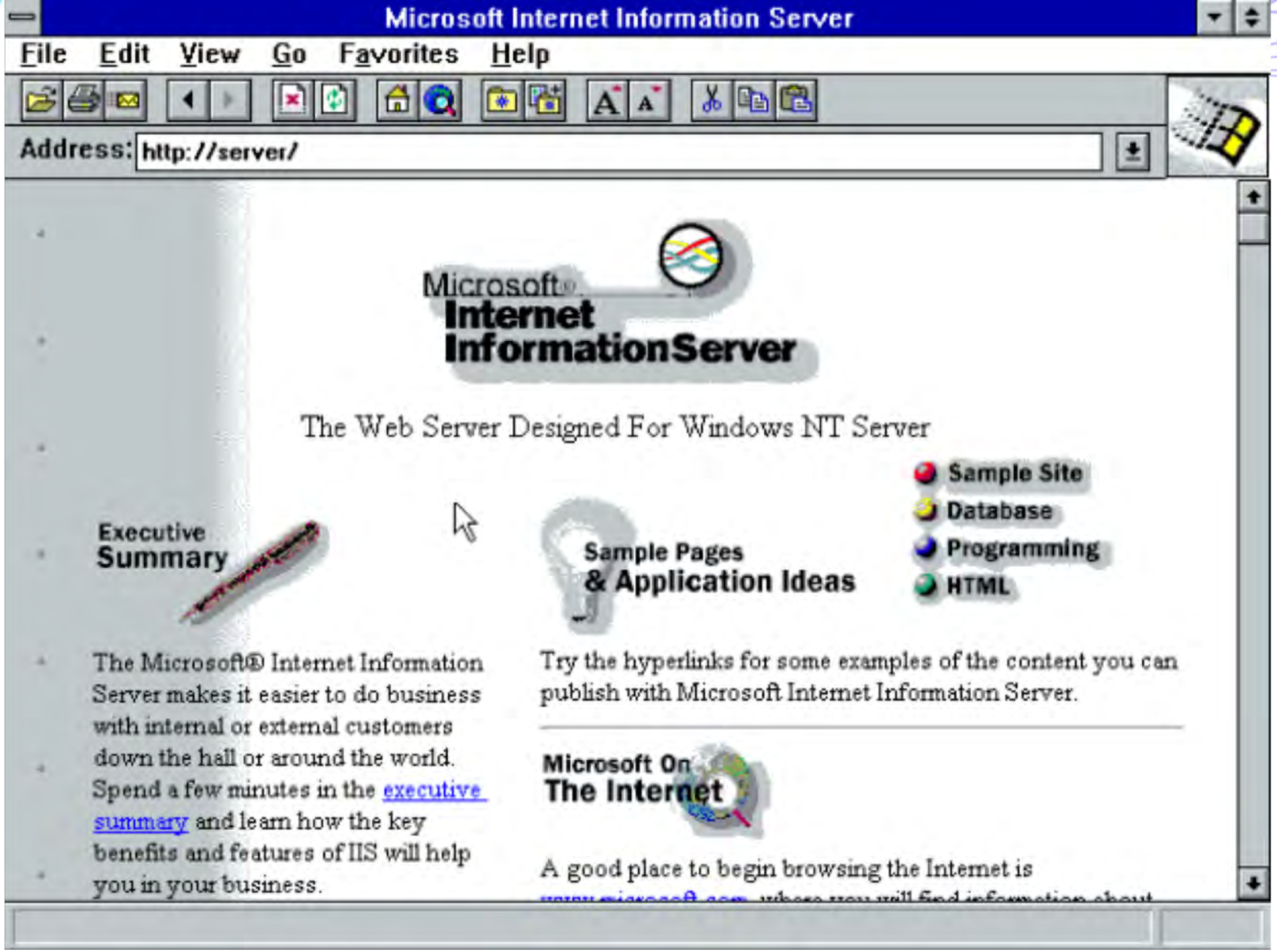
Chief Security Officer, Lookout
mmurray@lookout.com
Twitter: @mmurray


Those who do not learn from history…


Those who do not learn from history…
Are doomed to misunderstand the present.
(Apologies to Santayana)

In the beginning...


Netscape - [Gopher Menu]
File Edit View Go Bookmarks Options Directory Help
Back Forward Home Reload Images Open Print Find Stop
What's New! What's Cool! Upgrades Net Search Net Directory Newsgroups Handbook
Gopher Menu
Information About Gopher
Computer Information
Discussion Groups
Fun & Games
Internet file server (ftp) sites
Libraries
News
Other Gopher and Information Servers
Phone Books
Search Gopher Titles at the University of Minnesota
Search lots of places at the University of Minnesota
University of Minnesota Campus Information


Microsoft Internet Information Server
File Edit View Go Favorites Help
Address: http://server/
Microsoft Internet InformationServer
The Web Server Designed For Windows NT Server
Executive Summary
Sample Pages & Application Ideas
Sample Site
Database
Programming
HTML
The Microsoft® Internet Information Server makes it easier to do business with internal or external customers down the hall or around the world. Spend a few minutes in the executive summary and learn how the key benefits and features of IIS will help you in your business.
Try the hyperlinks for some examples of the content you can publish with Microsoft Internet Information Server.
Microsoft On The Internet
A good place to begin browsing the Internet is

November 6, 1996

.oO Phrack 49 Oo.

Volume Seven, Issue Forty-Nine

File 14 of 16

BugTraq, r00t, and Underground.Org
bring you

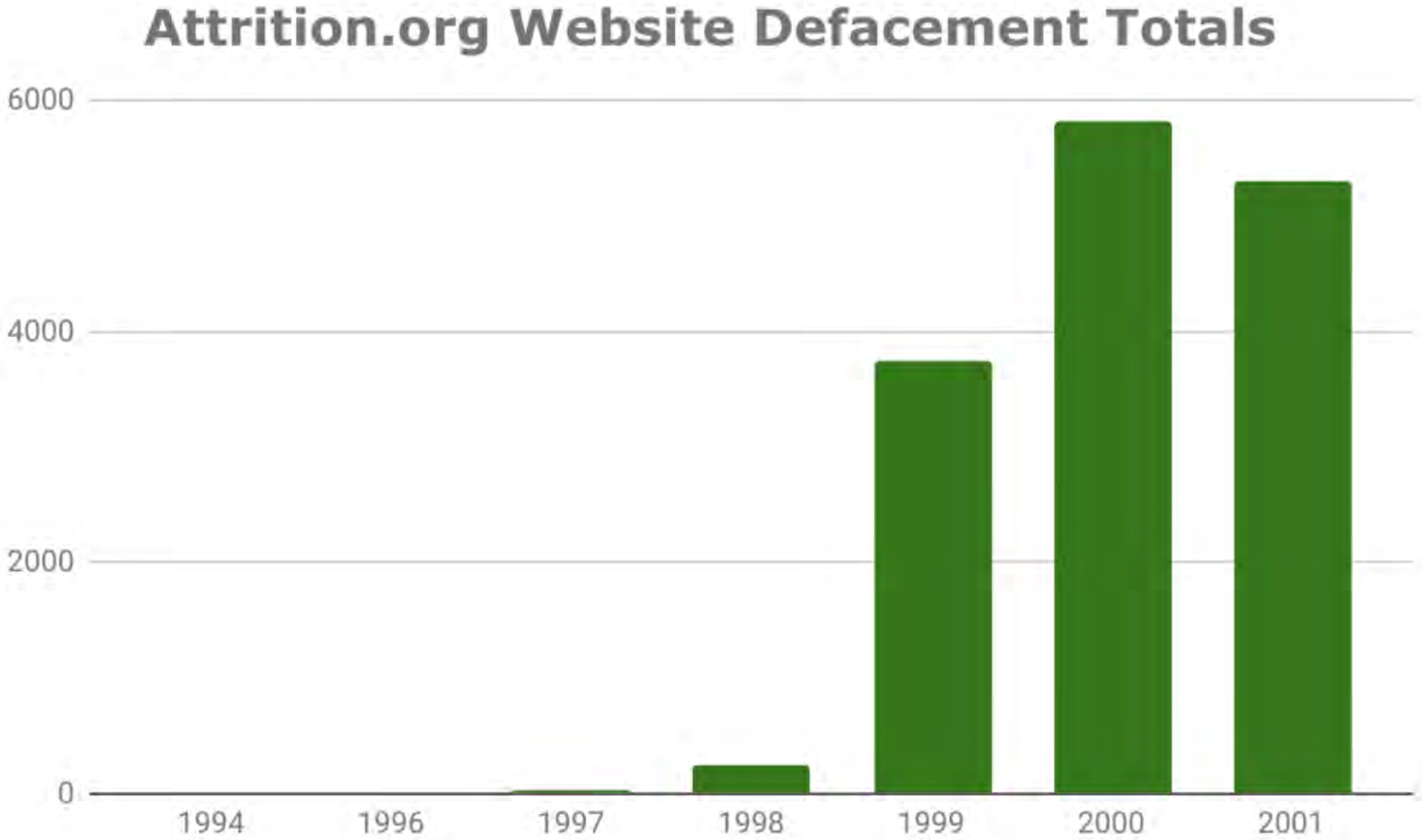
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Smashing The Stack For Fun And Profit
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

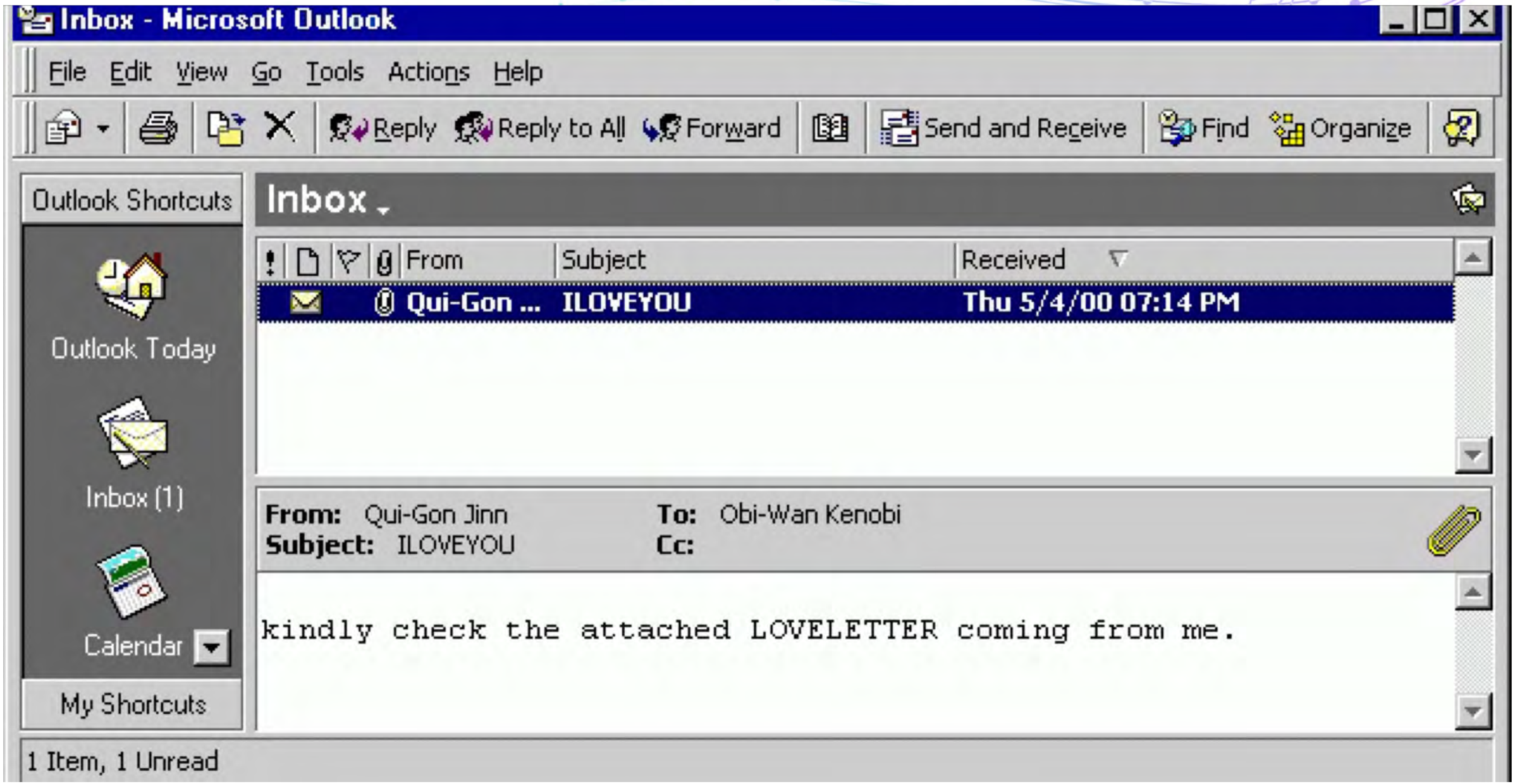
by Aleph One
aleph1@underground.org

`smash the stack` [C programming] n. On many C implementations it is possible to corrupt the execution stack by writing past the end of an array declared auto in a routine. Code that does this is said to smash the stack, and can cause return from the routine to jump to a random address. This can produce some of the most insidious data-dependent bugs known to mankind. Variants include trash the stack, scribble the stack, mangle the stack; the term mung the stack is not used, as this is never done intentionally. See spam; see also alias bug, fandango on core, memory leak, precedence lossage, overrun screw.

https://dl.packetstormsecurity.net/9911-exploits/msadc2.pl

```
#!/usr/bin/perl
#
# MSADC/RDS 'usage' (aka exploit) script version 2
#
#       by rain forest puppy
#
#       - added UNC support, really didn't clean up code, but oh well

use Socket; use Getopt::Std;
getopts("e:vd:h:XRVNwcu:s:", \%args);

print "-- RDS smack v2 - rain forest puppy / ADM / wiretrip --\n";

if (!defined $args{h} && !defined $args{R}) {
print qq~
Usage: msadc.pl -h <host> { -d <delay> -X -v }
        -h <host>               = host you want to scan (ip or domain)
        -d <seconds>            = delay between calls, default 1 second
        -X                      = dump Index Server path table, if available
        -N                      = query VbBusObj for NetBIOS name
        -V                      = use VbBusObj instead of ActiveDataFactory
        -v                      = verbose
        -e                      = external dictionary file for step 5
        -u <\\\\host\\share\\file>      = use UNC file
        -w                      = Windows 95 instead of Windows NT
        -c                      = v1 compatibility (three step query)
        -s <number>             = run only step <number>

        Or a -R will resume a (v2) command session

~; exit;}
```


Attrition.org Website Defacement Totals
6000
4000
2000
0
1994
1996
1997
1998
1999
2000
2001


Inbox - Microsoft Outlook
File Edit View Go Tools Actions Help
Reply Reply to All Forward Send and Receive Find Organize
Outlook Shortcuts
Outlook Today
Inbox (1)
Calendar
My Shortcuts
Inbox
From Subject Received
Qui-Gon ... ILOVEYOU Thu 5/4/00 07:14 PM
From: Qui-Gon Jinn To: Obi-Wan Kenobi
Subject: ILOVEYOU Cc:
kindly check the attached LOVELETTER coming from me.
1 Item, 1 Unread

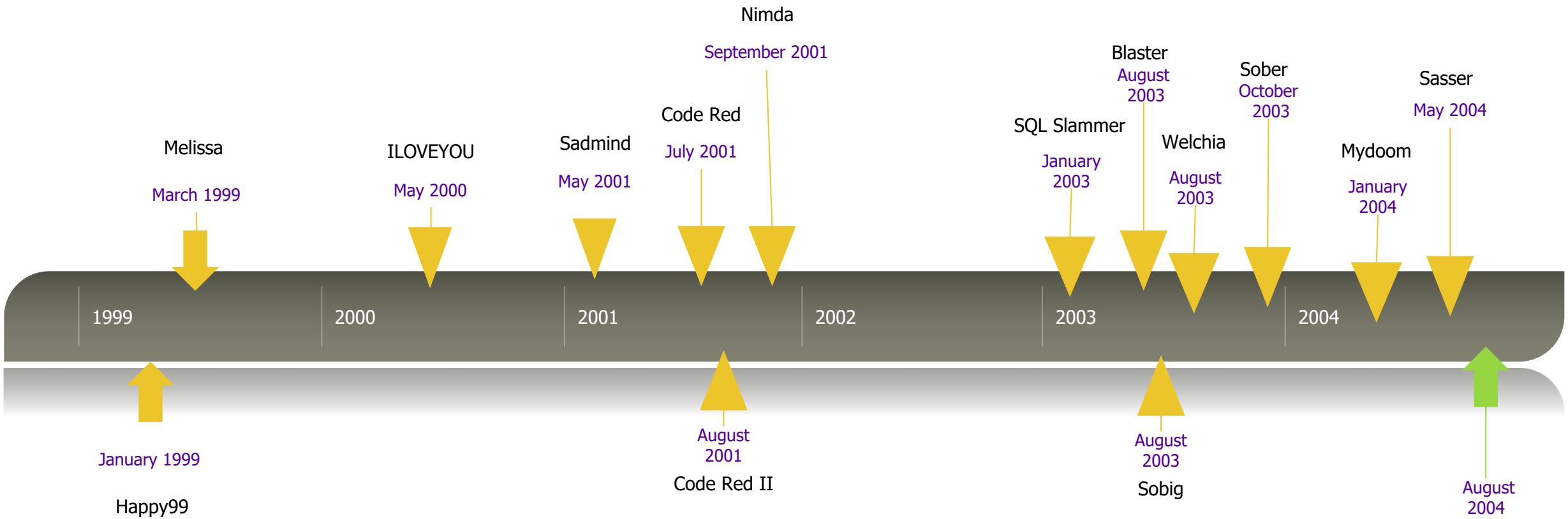
Networks: Hard & Crunchy on the Outside, Soft & Gooey on the Inside

January 25, 2003

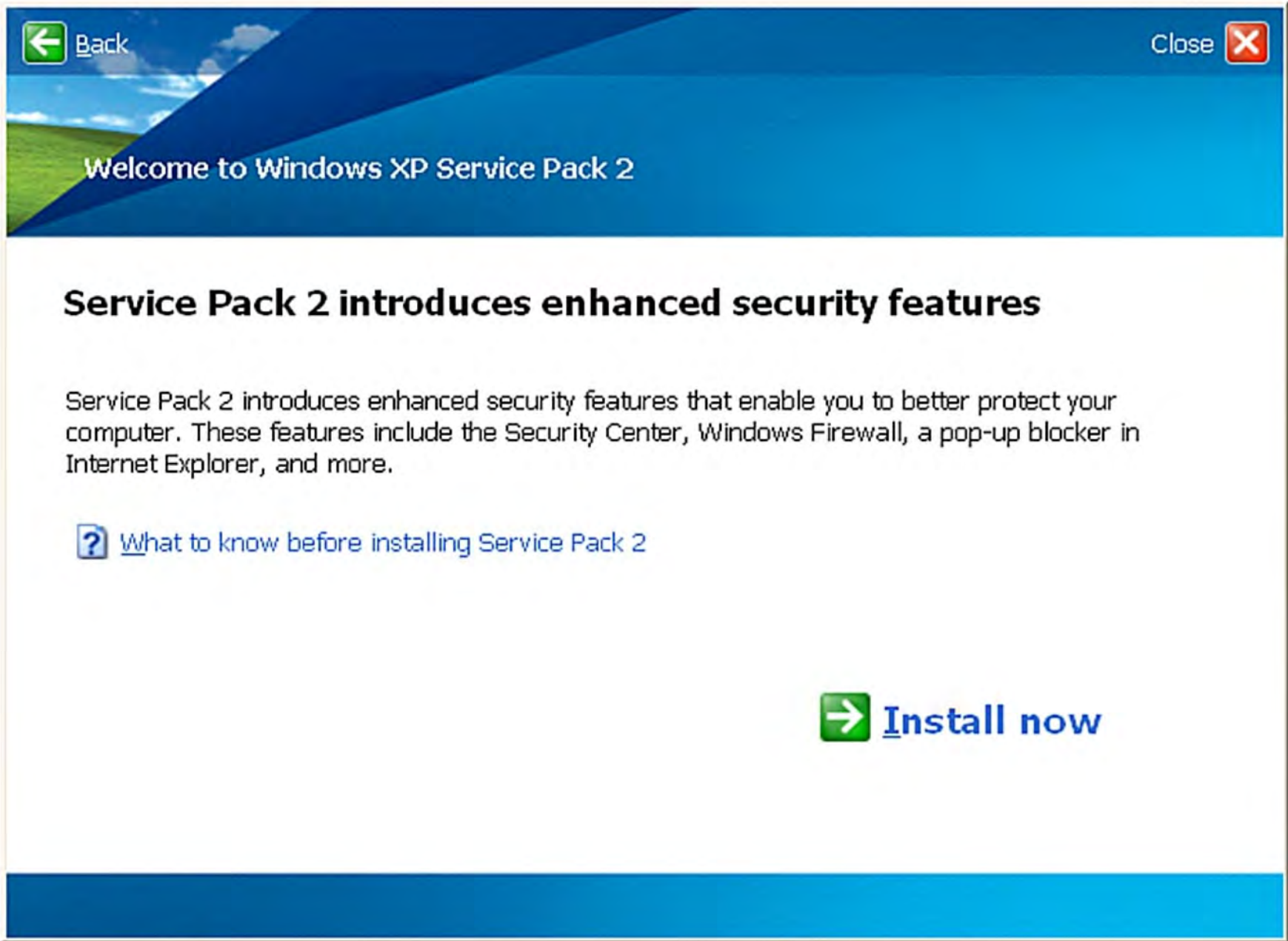
MS SQL WORM IS DESTROYING INTERNET BLOCK PORT 1434!

From: Michael Bacarella <mbac () netgraft com>
Date: Sat, 25 Jan 2003 02:11:41 -0500

```
I'm getting massive packet loss to various points on the globe.
I am seeing a lot of these in my tcpdump output on each
host.

02:06:31.017088 150.140.142.17.3047 > 24.193.37.212.ms-sql-m:  udp 376
02:06:31.017244 24.193.37.212 > 150.140.142.17: icmp: 24.193.37.212 udp port ms-sql-m unreachable [tos 0xc0

It looks like there's a worm affecting MS SQL Server which is
pingflooding addresses at some random sequence.

All admins with access to routers should block port 1434 (ms-sql-m)!

Everyone running MS SQL Server shut it the hell down or make
sure it can't access the internet proper!

I make no guarantees that this information is correct, test it
out for yourself!

--
Michael Bacarella                    24/7 phone: 646 641-8662
Netgraft Corporation                     http://netgraft.com/
      "unique technologies to empower your business"

Finger email address for public key.  Key fingerprint:
  C40C CB1E D2F6 7628 6308  F554 7A68 A5CF 0BD8 C055
```


Nimda
September 2001
Blaster
August 2003
Sober
October 2003
Sasser
May 2004
Code Red
July 2001
SQL Slammer
January 2003
Welchia
August 2003
Mydoom
January 2004
Melissa
March 1999
ILOVEYOU
May 2000
Sadmind
May 2001
1999
2000
2001
2002
2003
2004
January 1999
Happy99
August 2001
Code Red II
August 2003
Sobig
August 2004

August 25, 2004


Back
Close
Welcome to Windows XP Service Pack 2
Service Pack 2 introduces enhanced security features
Service Pack 2 introduces enhanced security features that enable you to better protect your computer. These features include the Security Center, Windows Firewall, a pop-up blocker in Internet Explorer, and more.
What to know before installing Service Pack 2
Install now

Jericho Forum: Deperimiterization

1. The scope and level of protection should be specific and appropriate to the asset at risk.
2. Security mechanisms must be pervasive, simple, scalable and easy to manage.
3. Assume context at your own peril.
4. Devices and applications must communicate through open, secure protocols.
5. All devices must be capable of maintaining their security policy on an un-trusted network.
6. All people, processes and technology must have declared and transparent levels of trust for any transaction to take place.
7. Mutual trust assurance levels must be determinable.
8. Authentication, authorization and accountability must interoperate/exchange outside of your locus/area of control.
9. Access to data should be controlled by security attributes of the data itself.
10. Data privacy (and security of any asset of sufficiently high value) requires a segregation of duties/privileges.
11. By default, data must be appropriately secured when stored, in transit, and in use.

The Creation of the Modern Internet

amazon web services

March 2006

Amazon re-launches AWS

June 2007

Apple releases iPhone

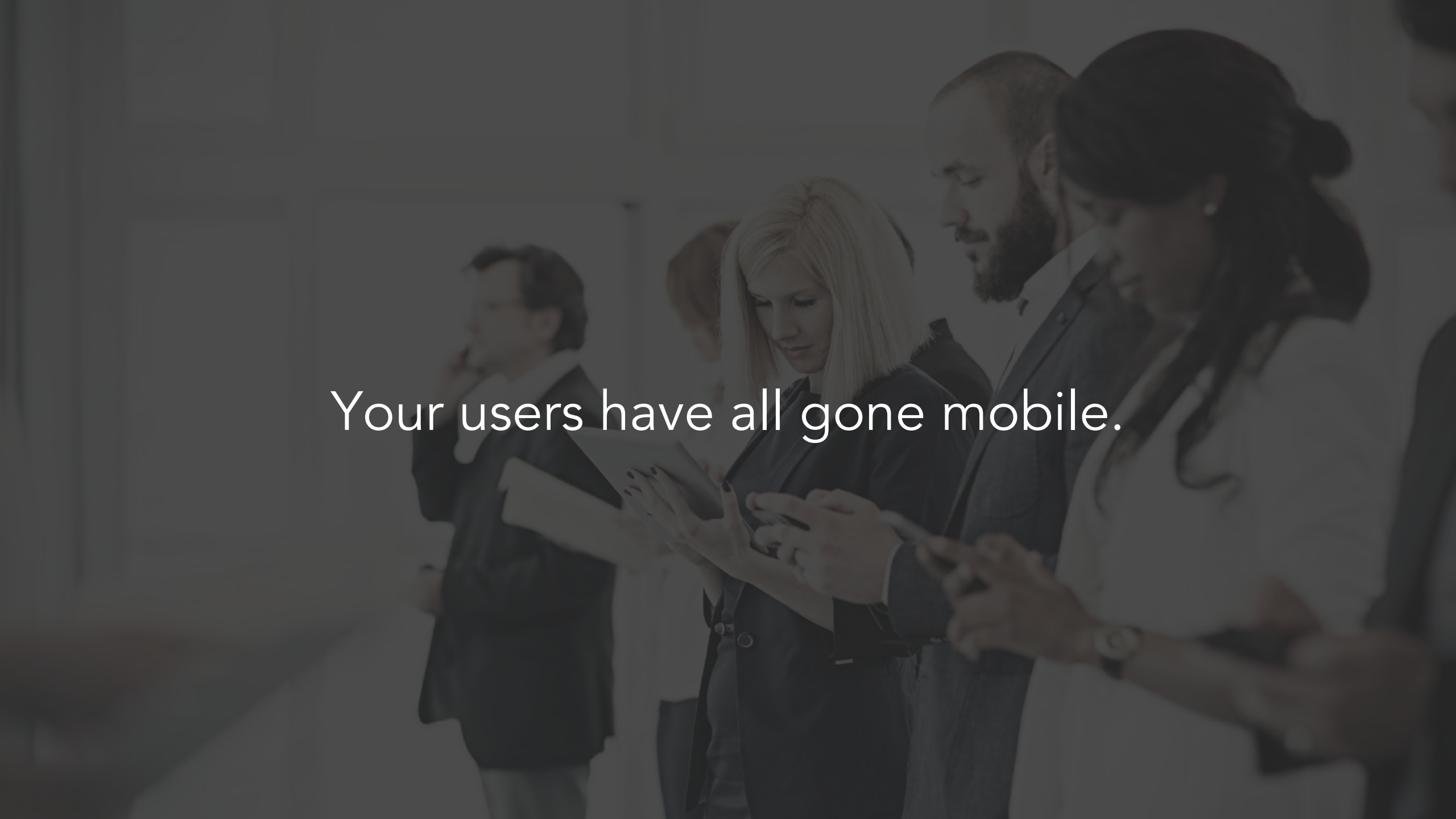
September 2008

Google releases Android

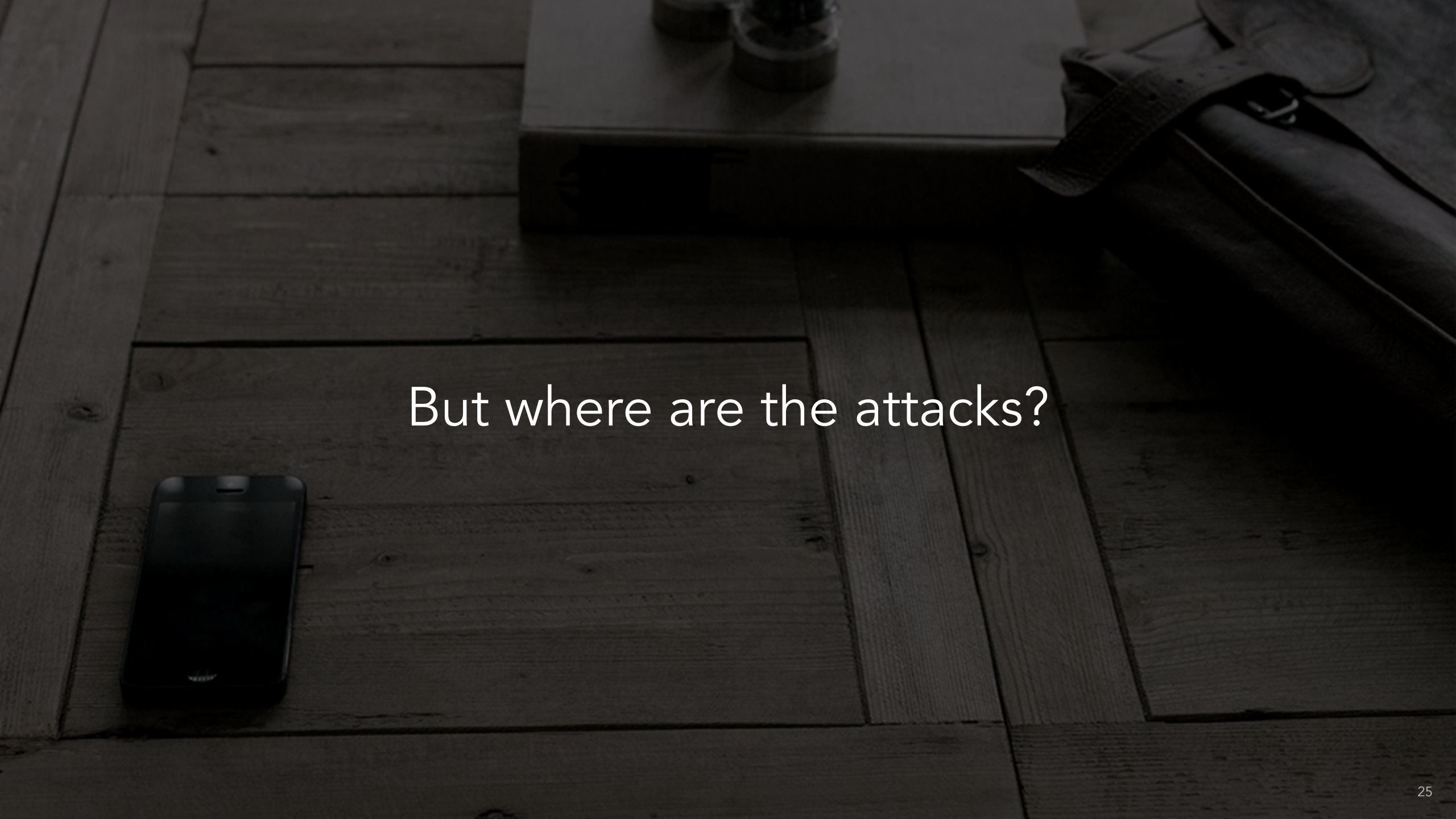
Fast forward to today...

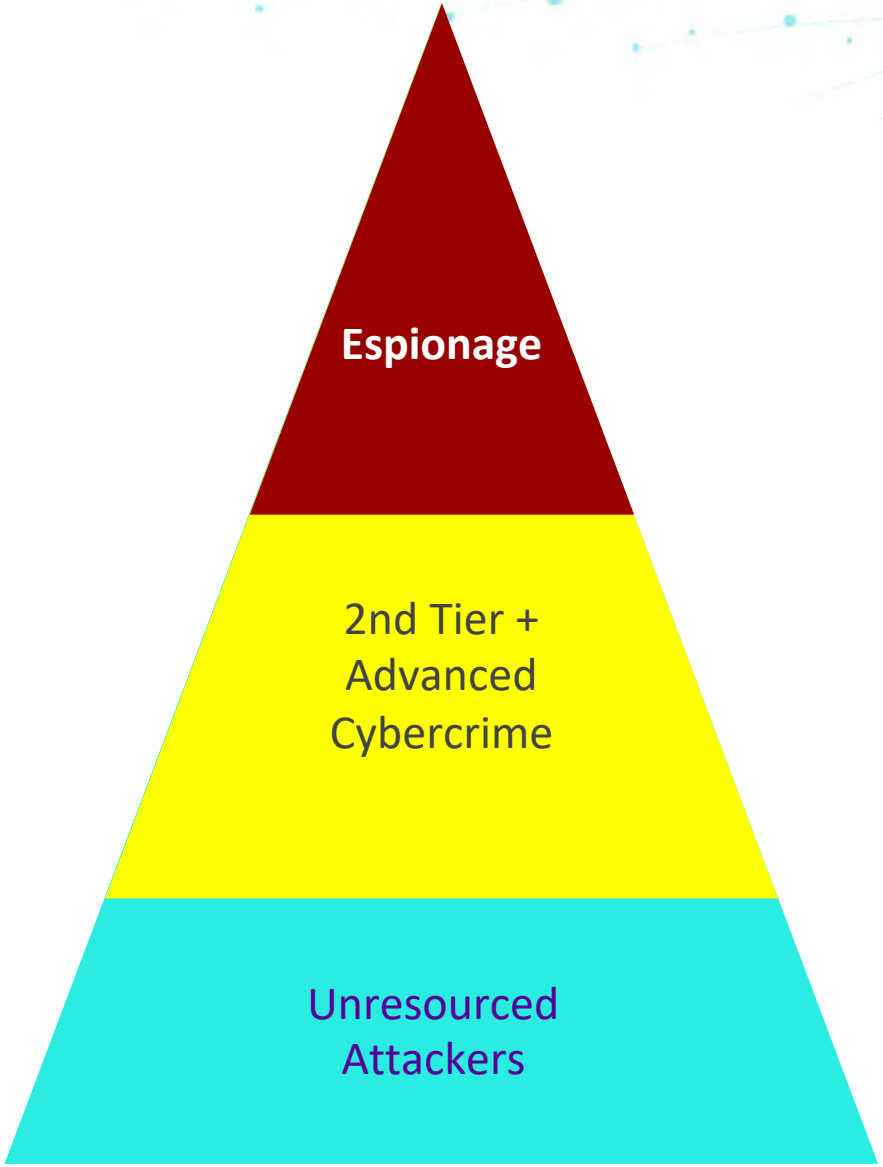

Your data center is in the cloud.


Starbucks is your new enterprise Wi-Fi.


Your users have all gone mobile.

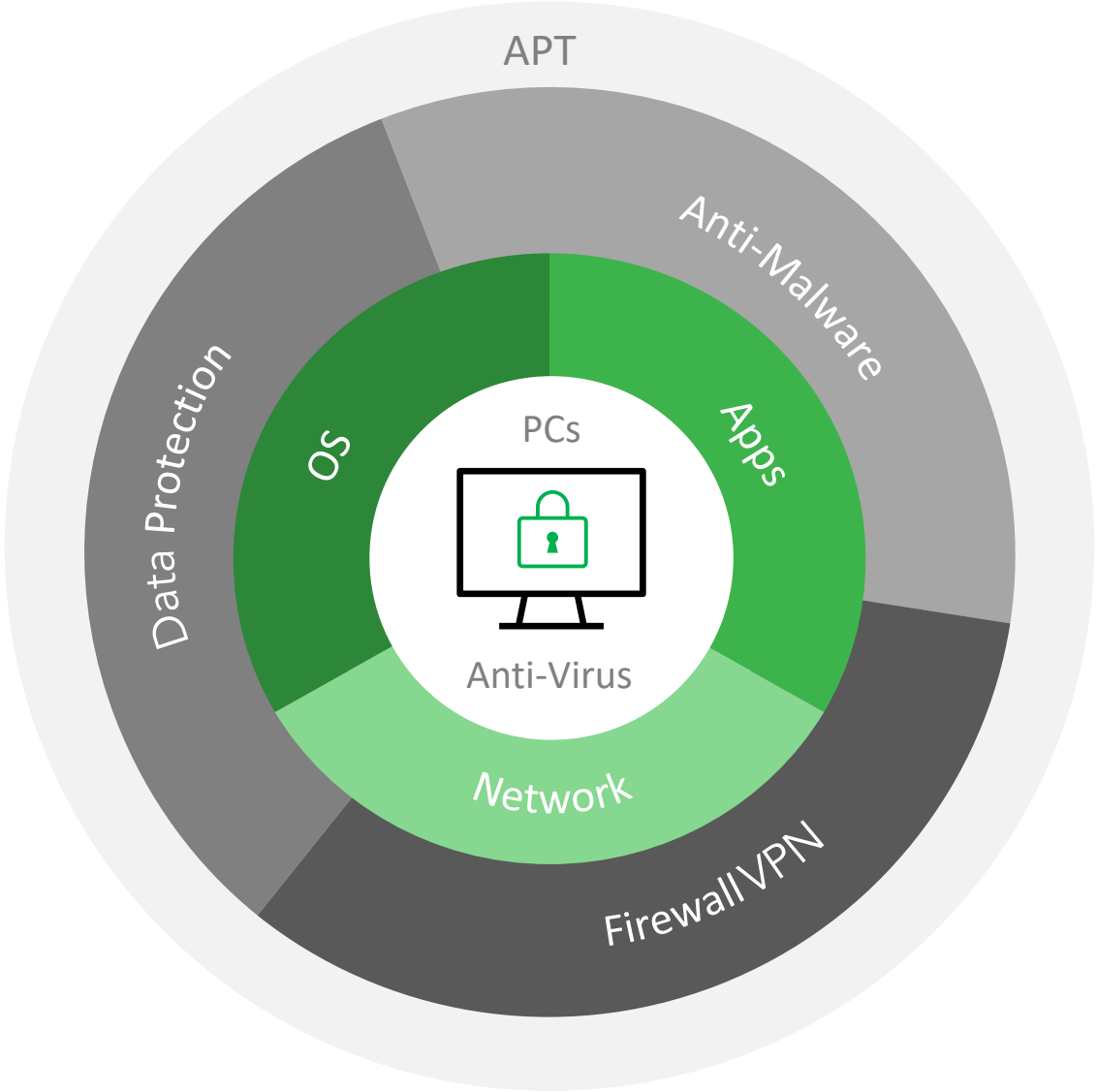

Your perimeter is gone.

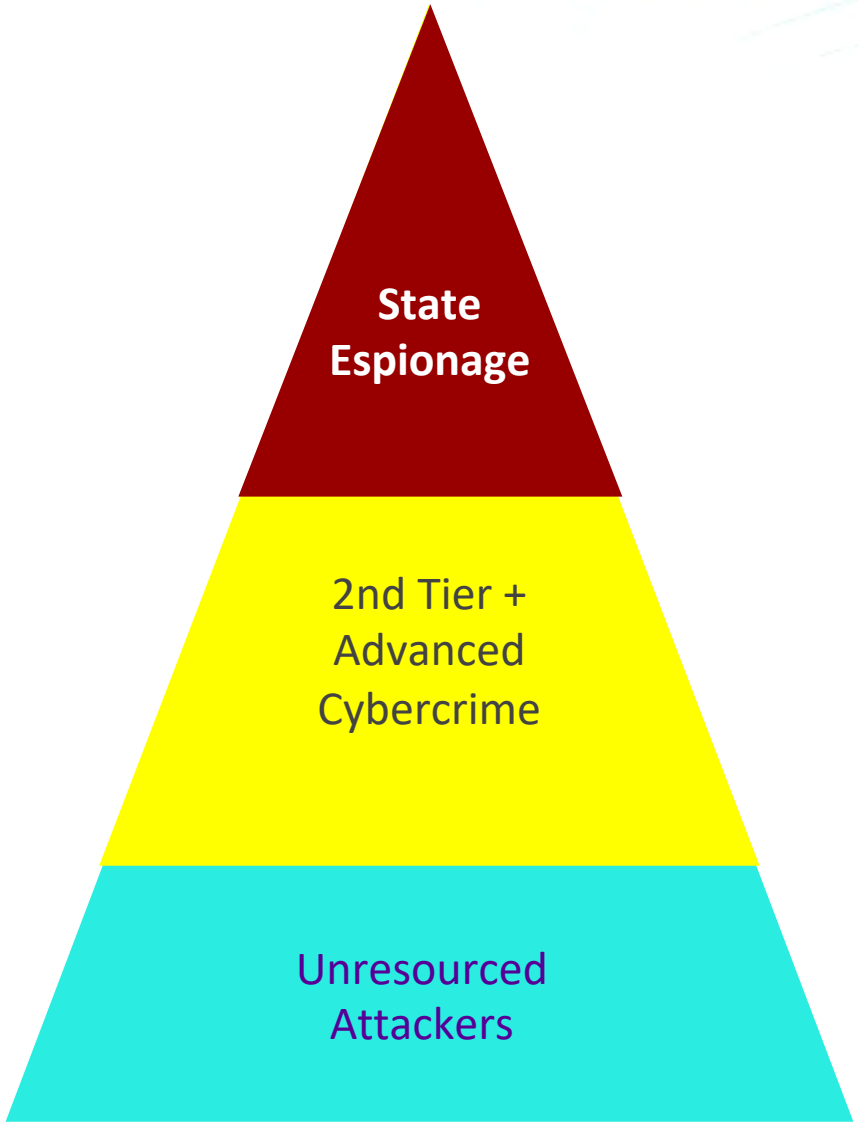

But where are the attacks?



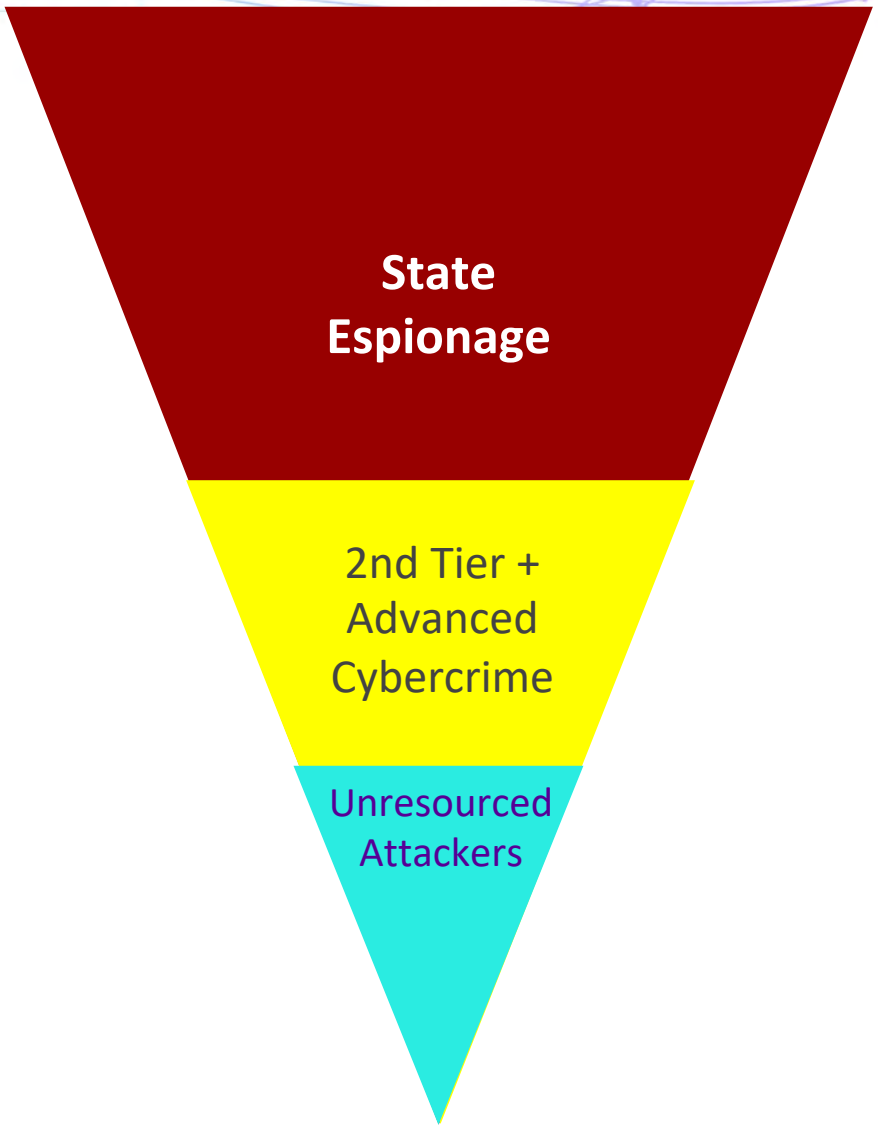
Original Computer Threat Landscape

The Evolution of Computer Security





Original Computer Threat Landscape



Mobile Threat Landscape

TECH

Mobile-Phone Malware Is Rising. Blame Spies.

Contractors and companies are selling cheap spyware to repressive regimes around the world

By Robert McMillan

28 COMMENTS

June 7, 2018 7:00 a.m. ET

Spies are increasingly hacking into the smartphones of political opponents and dissidents around the world, security researchers say, giving them access to data far more sensitive than what most people keep on personal computers.

Mobile-security firm Lookout Inc. counted 22 phone-hacking efforts in the first five months of this year that appeared to be government-backed. Most targeted political opponents in developing nations, Lookout said. The company's researchers identified just two such efforts in all of 2015.

The increase is being driven by the proliferation both of low-cost smartphones and of companies selling spyware and hacking tools to access them, said Claudio Guarnieri, a security researcher with the human-rights group Amnesty International. Most hacking efforts now target mobile phones, Mr. Guarnieri said, while in 2015 the majority still involved personal computers.

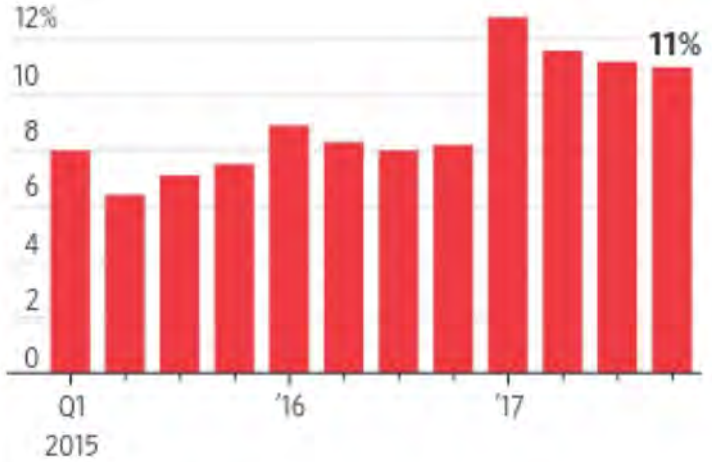
"It is one thing to compromise someone's computer," said Mike Murray, Lookout's vice president of security research. "It's another thing to have a listening device that they carry around with them 24 hours a day,"

The government-sponsored surveillance of mobile phones comes as more hackers of all stripes gain access to the devices. Turned against their owners, the phones can become powerful espionage tools, researchers say. Spies can monitor a user's contacts, communications, travel history and even their financial transactions.

Handheld Hacks

State-sponsored phone hacking is increasing as the smartphone becomes a bigger target.

Percentage of mobile phones world-wide infected with malicious software



State-linked mobile malware campaigns

Sources: McAfee (infections); Lookout (campaigns)

Lookout

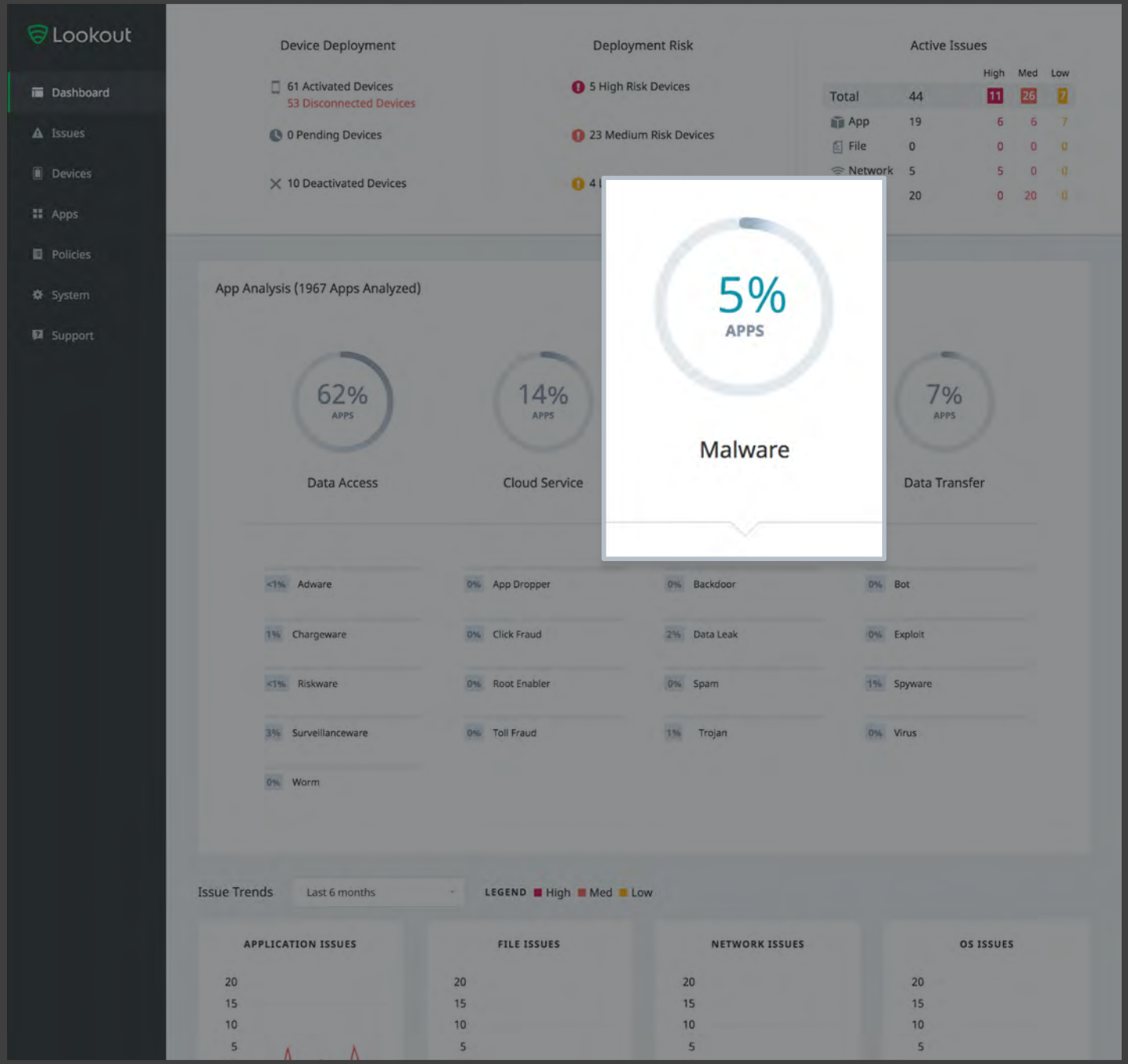
Reference: https://www.wsj.com/articles/mobile-phone-malware-is-rising-blame-spies-1528369200, June 7 2018

The Perfect Espionage Platform

Every nation-state attacker has a mobile espionage capability

Always Connected

- Voice
- Camera
- Email
- Location
- Passwords
- Contact lists
- and more…


Lookout
Dashboard
Issues
Devices
Apps
Policies
System
Support
Device Deployment
61 Activated Devices
53 Disconnected Devices
0 Pending Devices
10 Deactivated Devices
Deployment Risk
5 High Risk Devices
23 Medium Risk Devices
Active Issues
High Med Low
Total 44 11 26 7
App 19 6 6 7
File 0 0 0 0
Network 5 5 0 0
20 0 20 0
App Analysis (1967 Apps Analyzed)
62% APPS
Data Access
14% APPS
Cloud Service
5% APPS
Malware
7% APPS
Data Transfer
<1% Adware
0% App Dropper
0% Backdoor
0% Bot
1% Chargeware
0% Click Fraud
2% Data Leak
0% Exploit
<1% Riskware
0% Root Enabler
0% Spam
1% Spyware
3% Surveillanceware
0% Toll Fraud
1% Trojan
0% Virus
0% Worm
Issue Trends
Last 6 months
LEGEND High Med Low
APPLICATION ISSUES
FILE ISSUES
NETWORK ISSUES
OS ISSUES
20
15
10
5

RSAConference2019

Identity is the New Perimeter

Mobile APT Kill Chain

Phishing

- Email
- SMS / Text
- Social media

Gain Access

- Dropper installs, or
- Exploit, or
- Victim clicks thru for install

Elevate Privilege

- Install payload or
- Dropped apps, or
- Exploit vulns

Perform Espionage

Receive commands to:

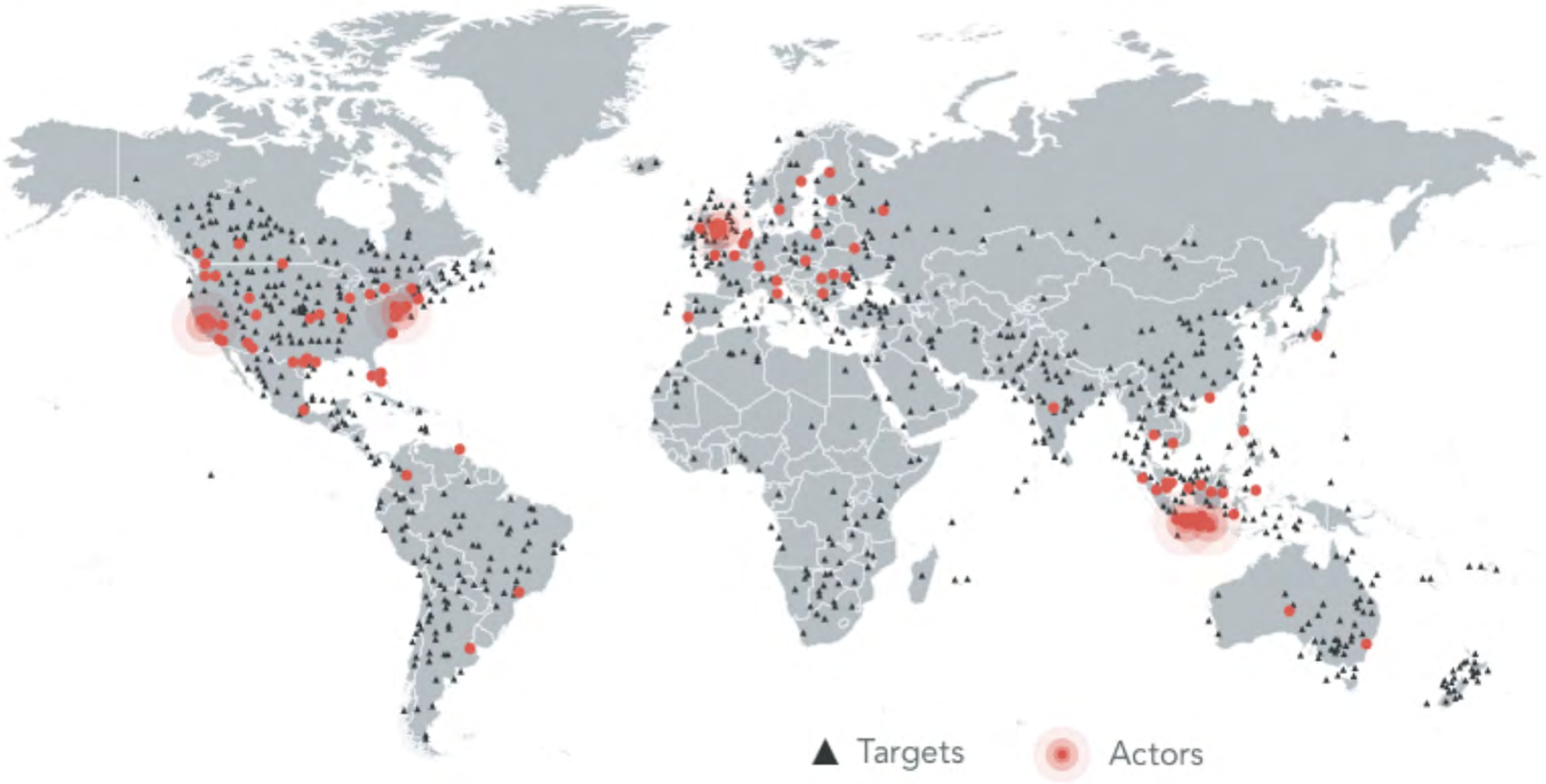
- Send / exfiltrate private data, pictures, camera, audio
- Steal credentials

Actions on Objectives

With victim's identity and access rights:

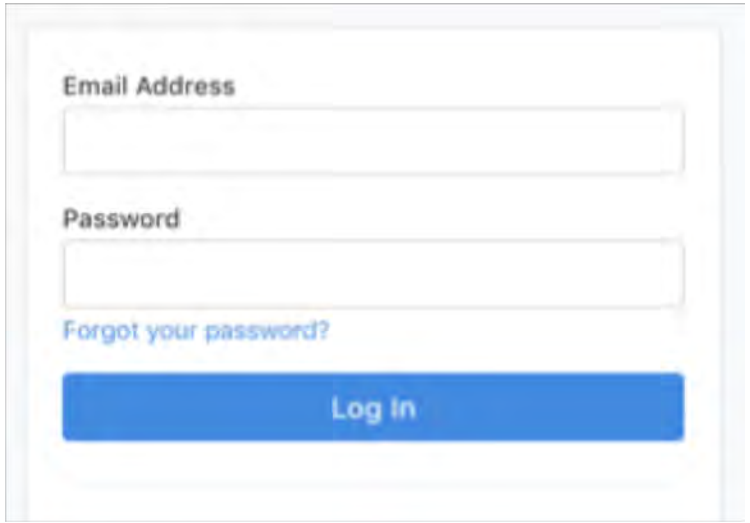
- Access enterprise data
- Access cloud services

Leebo Phishing Kit Proliferation



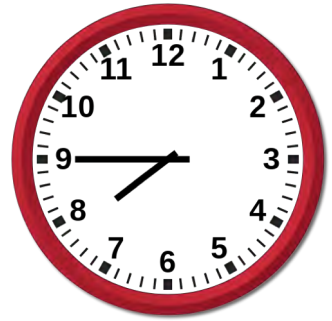
Case Study: DNC Phishing

How APTs go from 0-60 in a few hours



Not Secure | accounts.ngpvan.verifyauth.com

Success! The example.com server block is working!



Secure | https://accounts.ngpvan.verifyauth.com

- Email Address
- Password

Caps Lock is on.

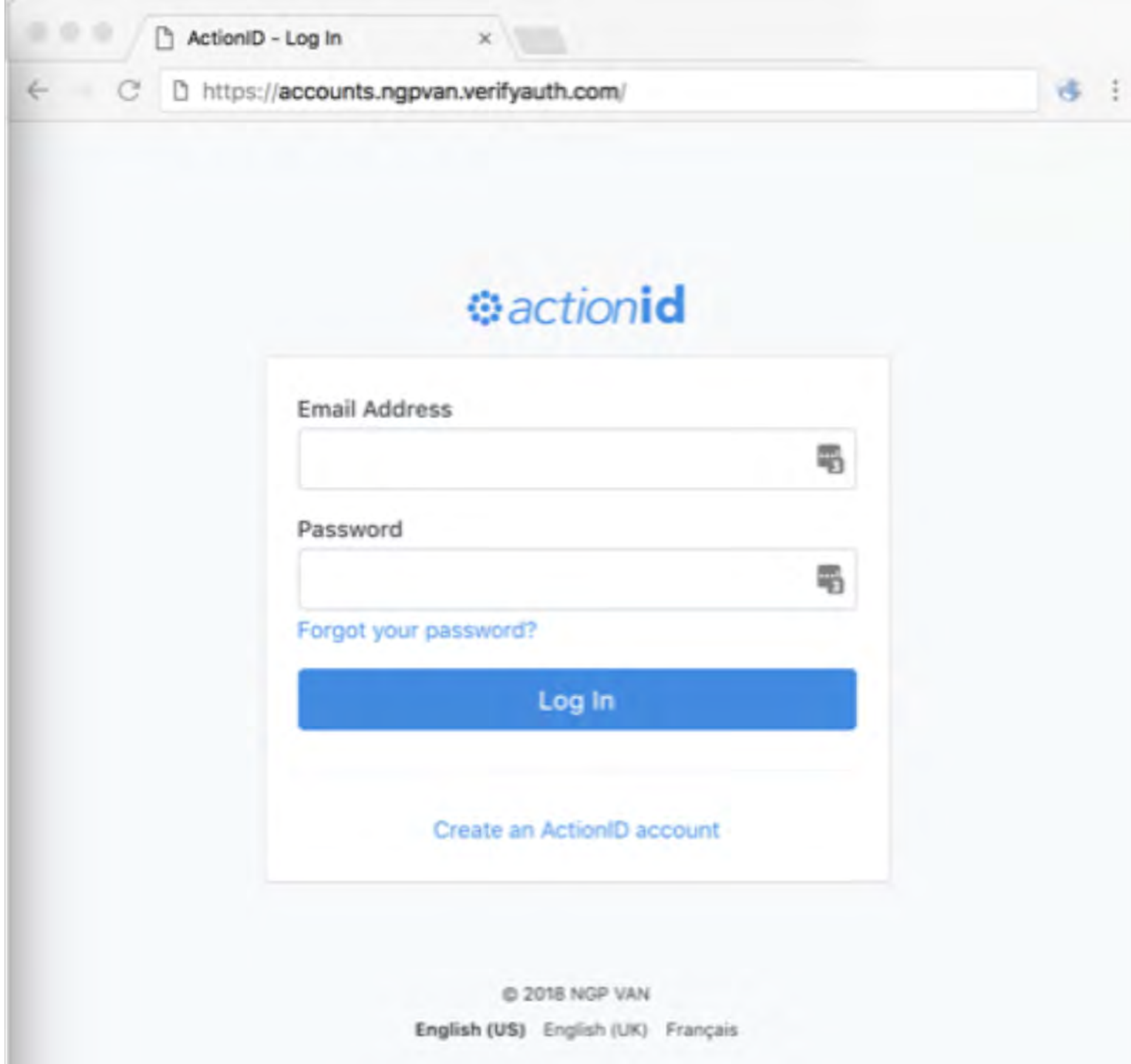
- Forgot your password?

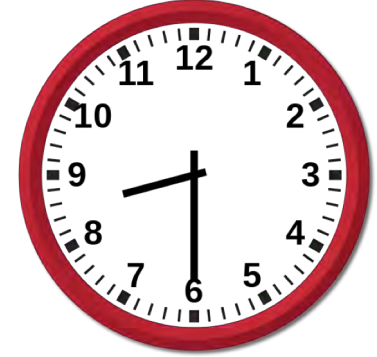
Log In

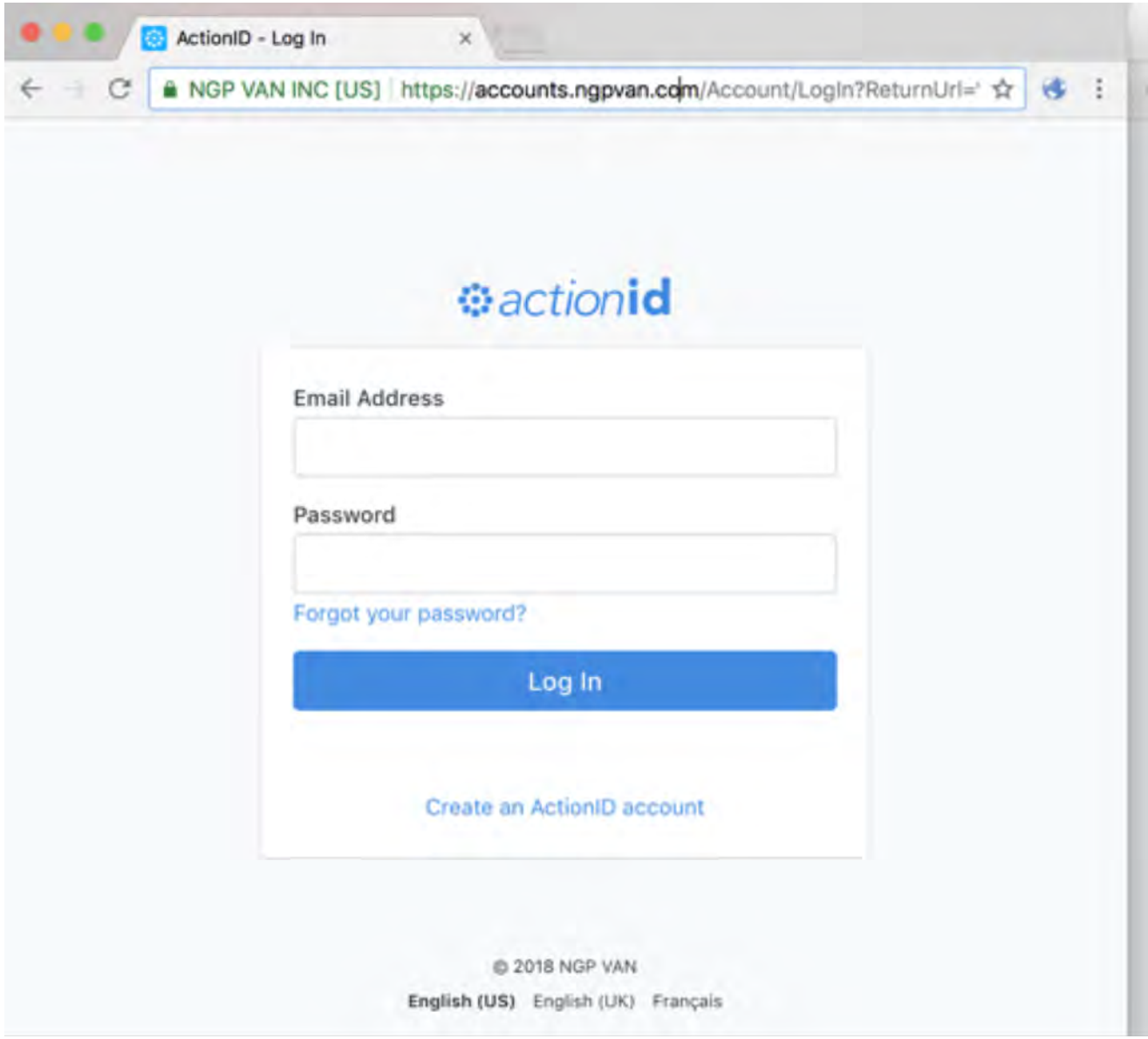
Create an ActionID account

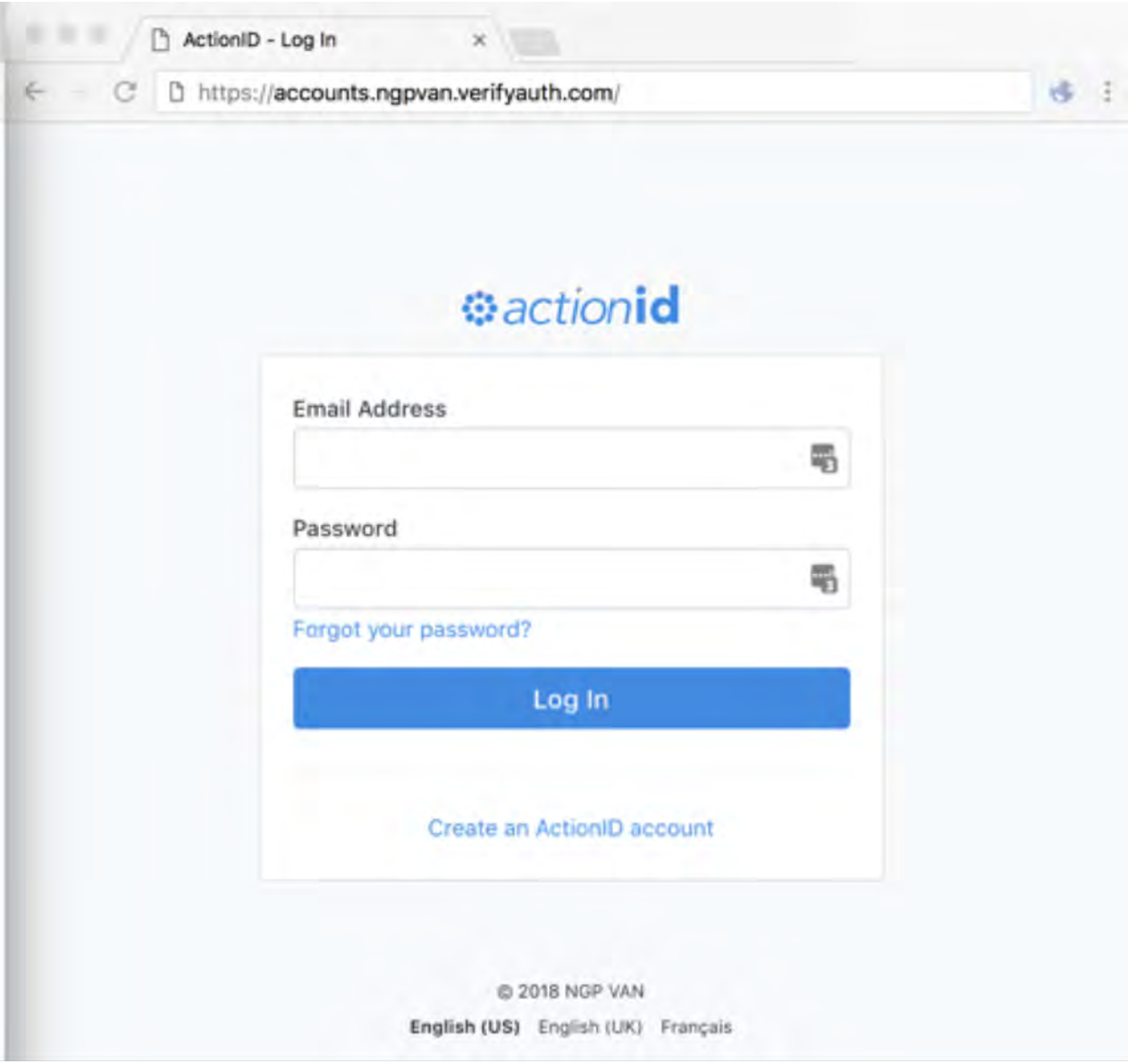
Submit

- English (US)
- English (UK)
- Français


ActionID - Log In
https://accounts.ngpvan.verifyauth.com/
actionid
Email Address
Password
Forgot your password?
Log In
Create an ActionID account
© 2018 NGP VAN
English (US) English (UK) Français

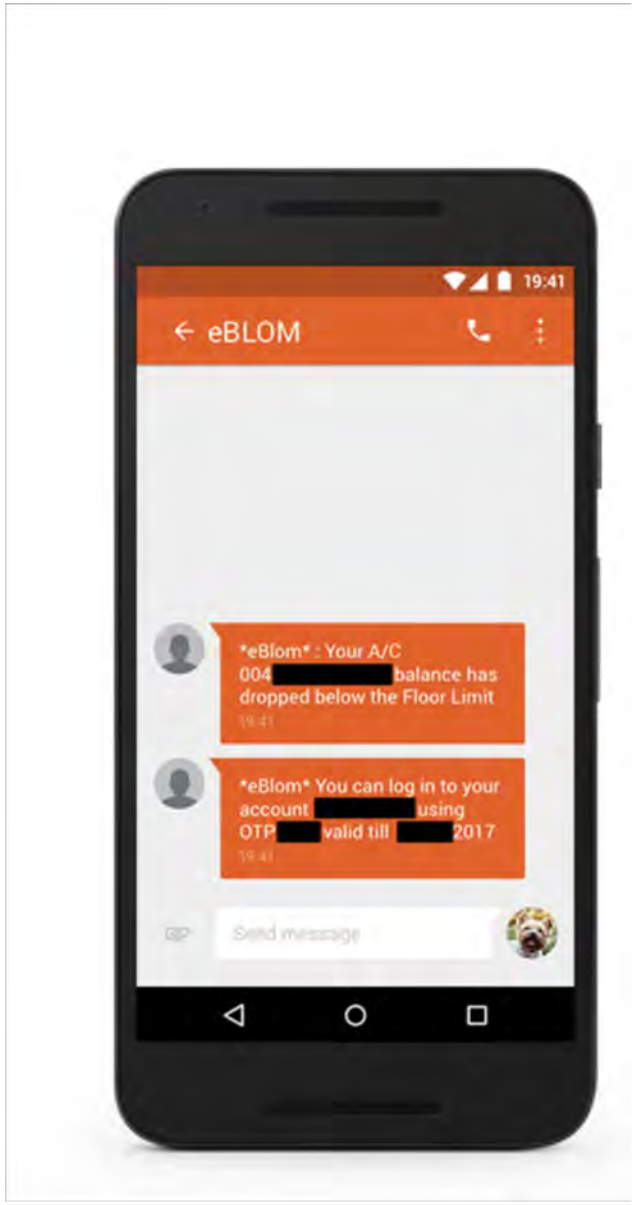

12
1
2
3
4
5
6
7
8
9
10
11

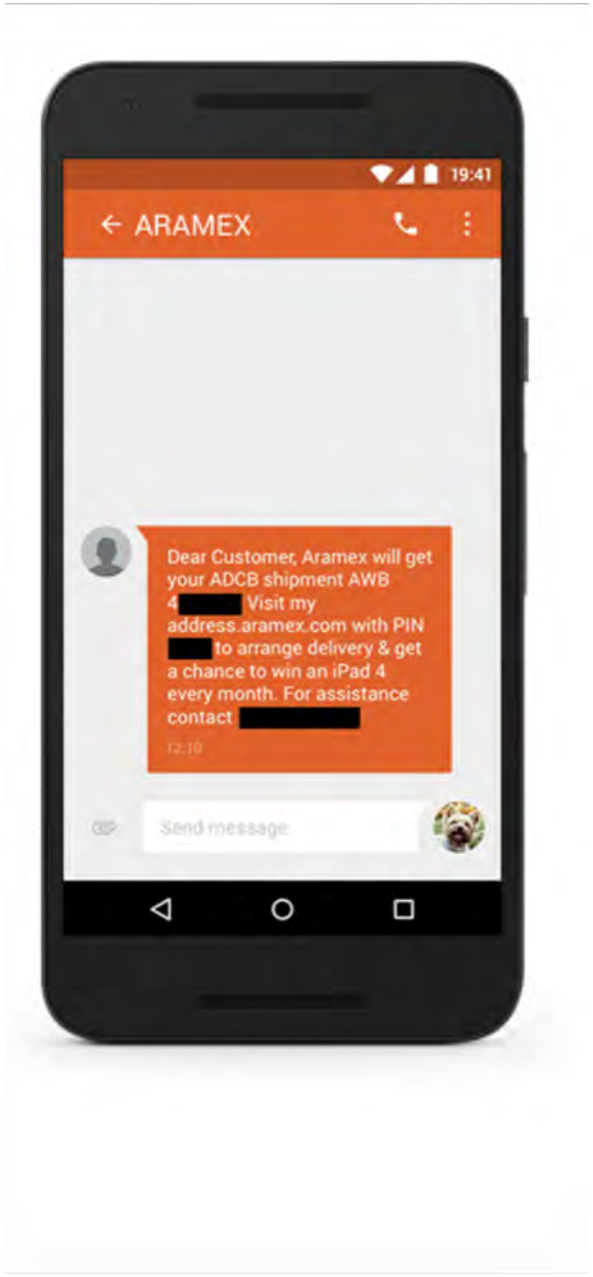

ActionID - Log In
NGP VAN INC [US] | https://accounts.ngpvan.com/Account/LogIn?ReturnUrl=
actionid
Email Address
Password
Forgot your password?
Log In
Create an ActionID account
© 2018 NGP VAN
English (US) English (UK) Français

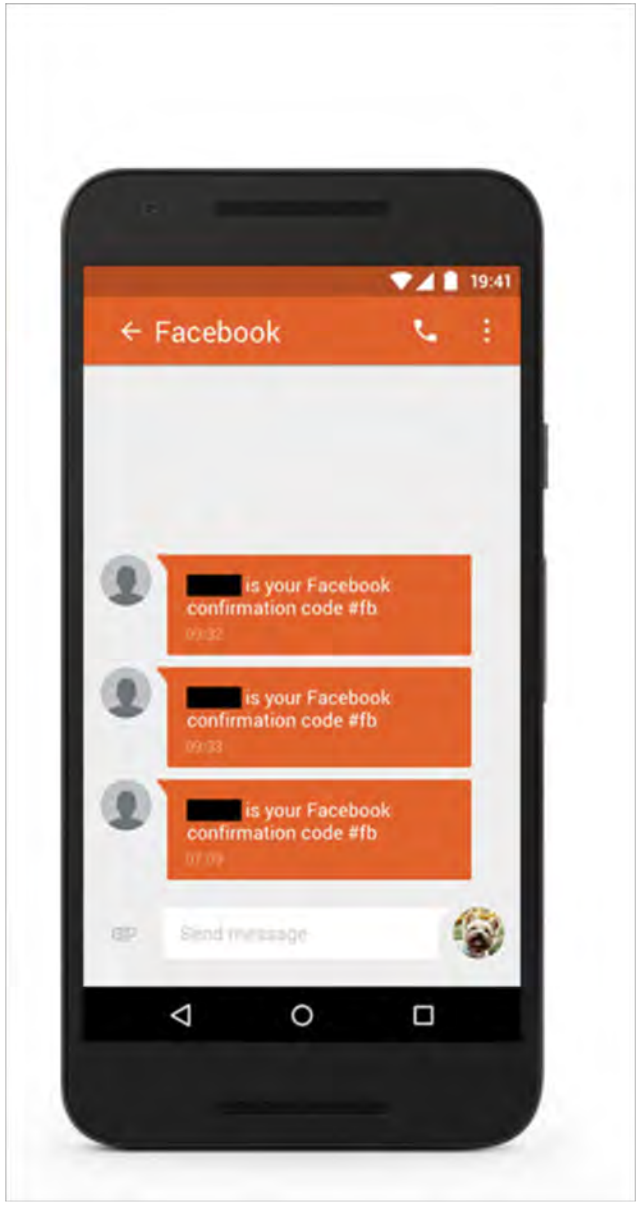

ActionID - Log In
https://accounts.ngpvan.verifyauth.com/
actionid
Email Address
Password
Forgot your password?
Log In
Create an ActionID account
© 2018 NGP VAN
English (US) English (UK) Français

Case Study: Dark Caracal

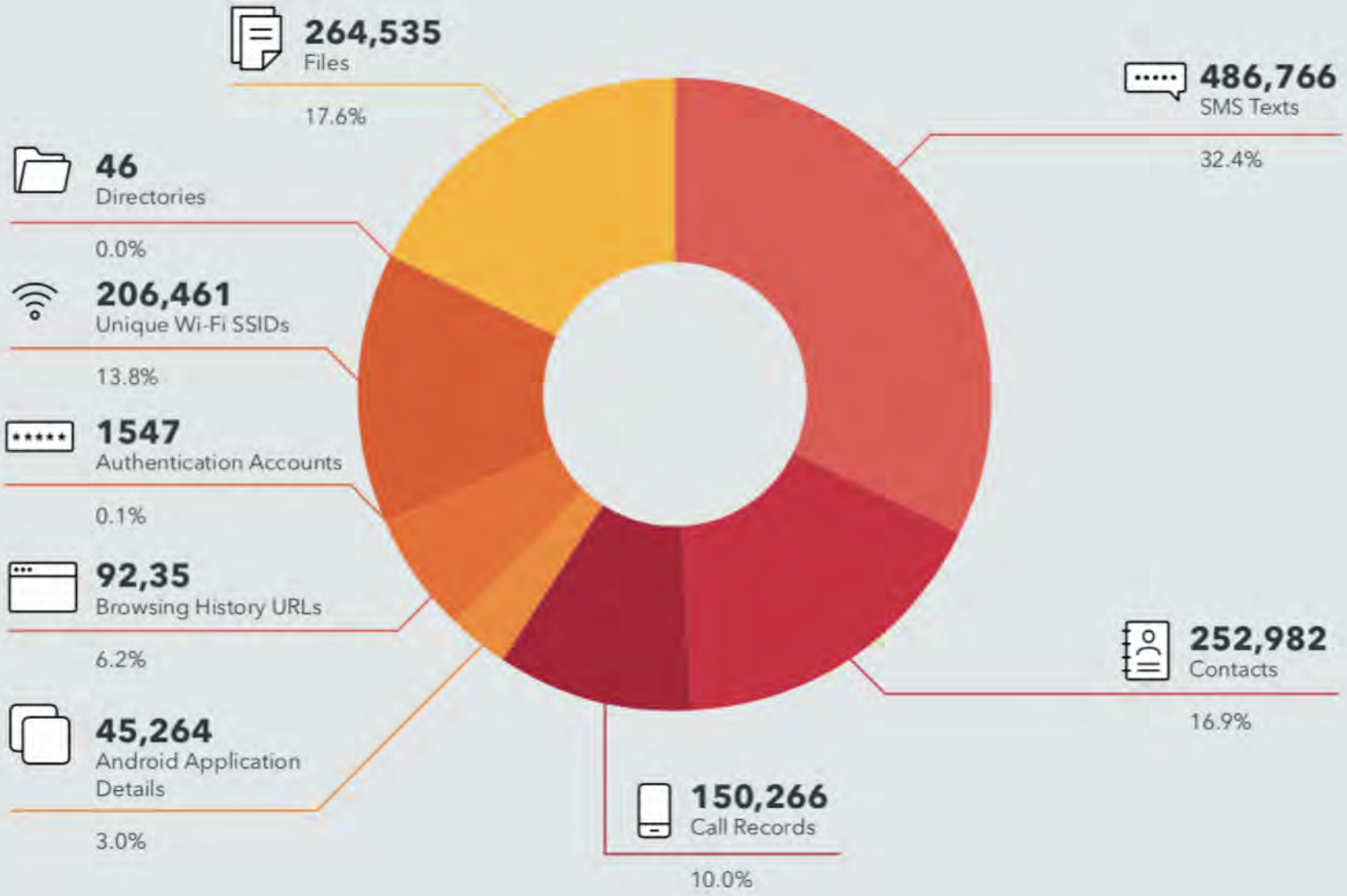
Cheap and Easy Cyber-espionage at a Global Scale


19:41
eBLOM
eBlom : Your A/C 004 balance has dropped below the Floor Limit
eBlom You can log in to your account using OTP valid till 2017
Send message


19:41
ARAMEX
Dear Customer, Aramex will get your ADCB shipment AWB 4 Visit my address.aramex.com with PIN to arrange delivery & get a chance to win an iPad 4 every month. For assistance contact
Send message


19:41
Facebook
is your Facebook confirmation code #fb
is your Facebook confirmation code #fb
is your Facebook confirmation code #fb
Send message

An overview of exfiltrated data from the Android campaigns can be seen in the figure below.



secureandroid.info/androidapps/index.html

android


Home


Whatsapp +


Telegram +


Threema +


Primo +


Signal +


Psiphon +

Tor +

Welcome To Our BlackMarket

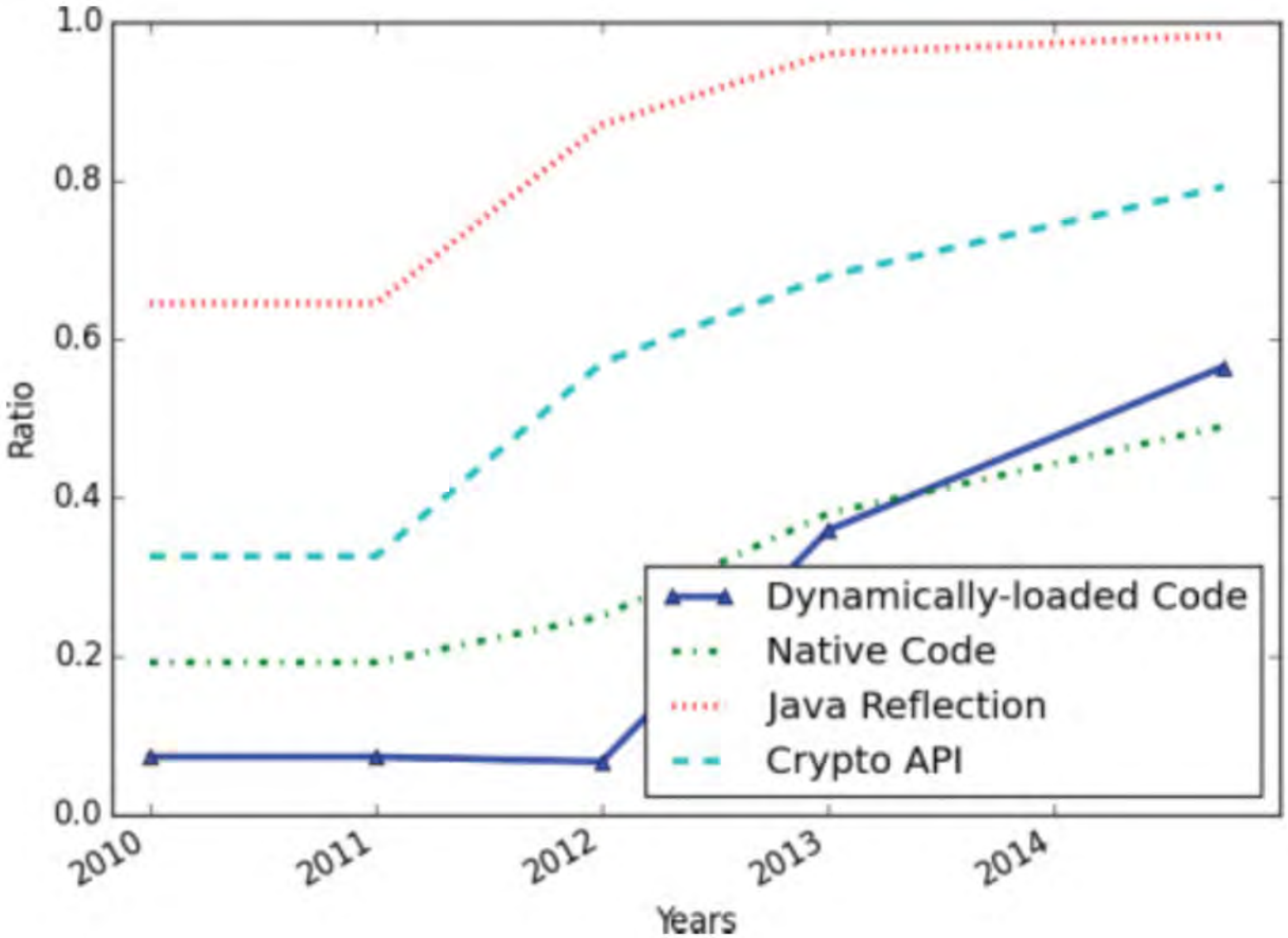
Quality is better than the original! Highly detailed, enhanced and enchanted miniatures. Powered up and flawless.

Home | Contact-us


Campus France Liban
National Museum
of Beirut

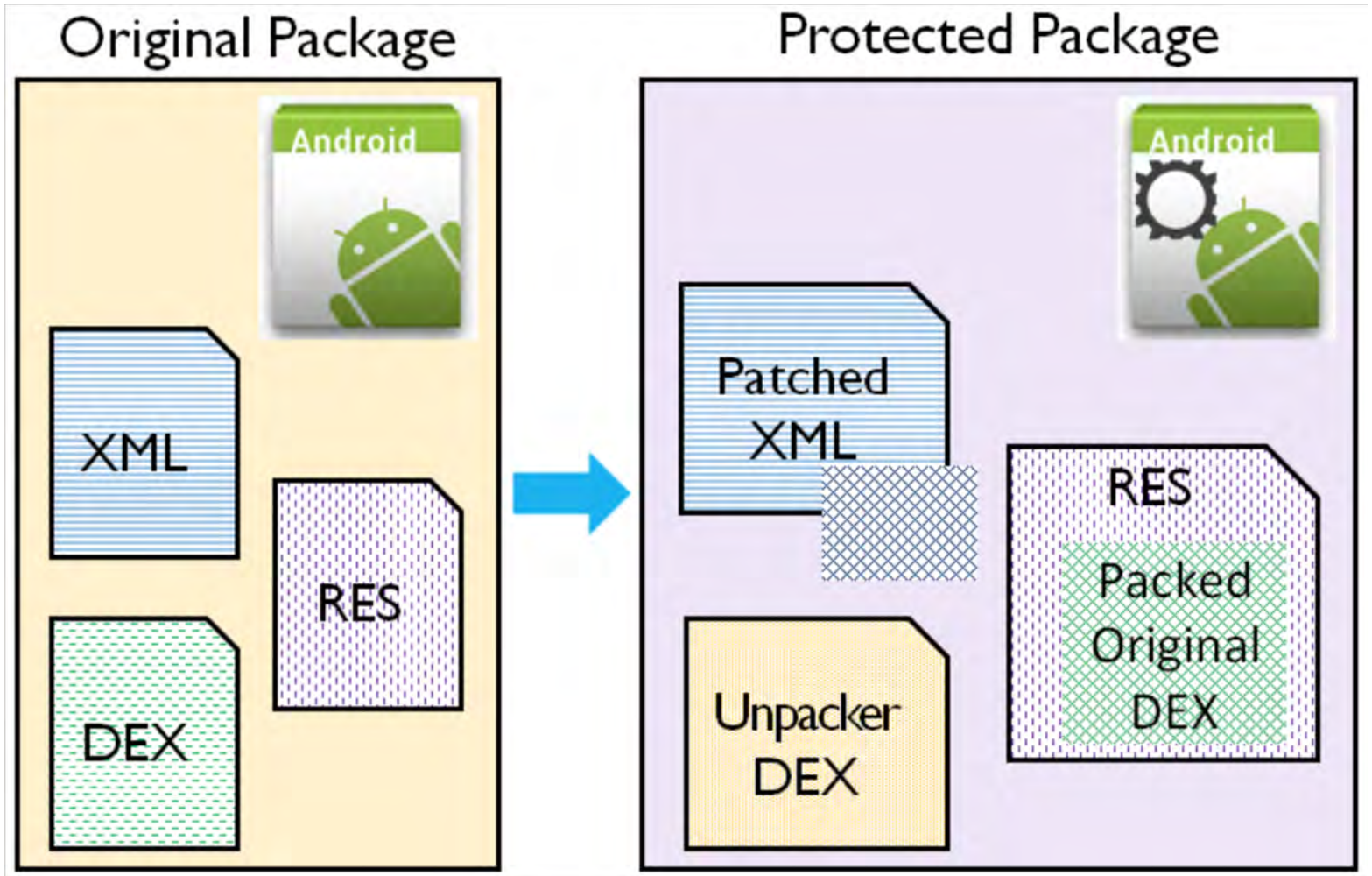
RSAConference2019

Mobile Threats beginning to Evolve



Lookout®

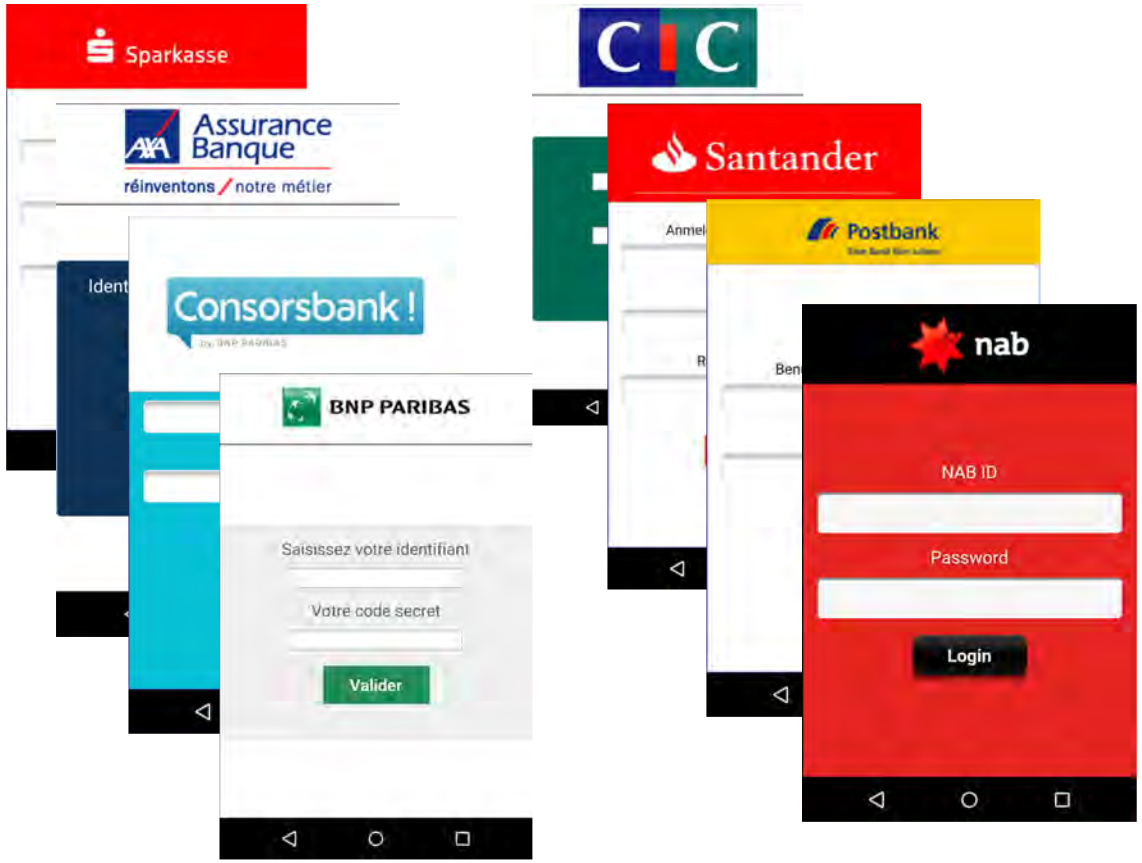
Source: https://dl.acm.org/citation.cfm?id=3017427



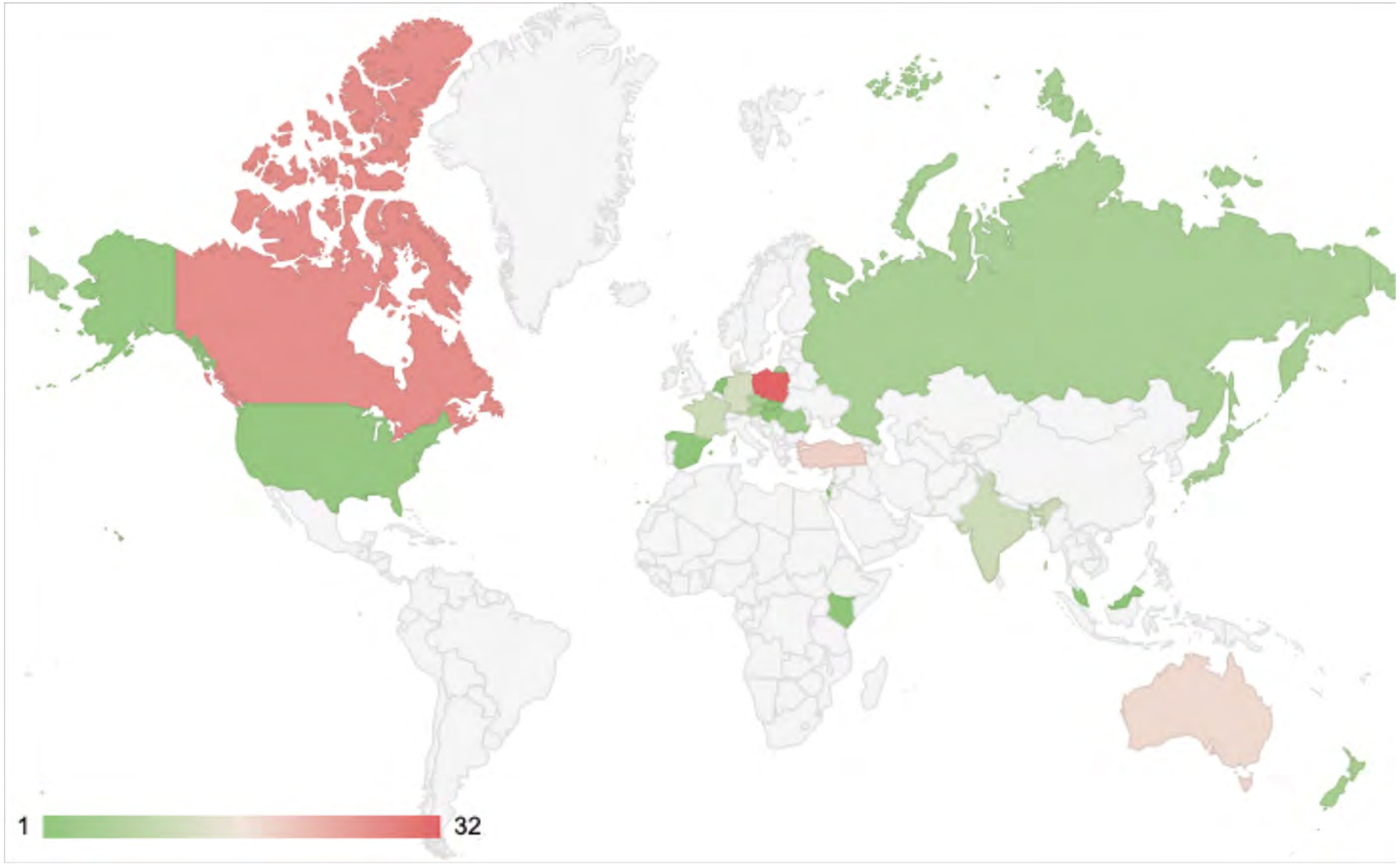
Source: https://raw.githubusercontent.com/ZSShen/Android-Code-Morph/master/res/AndroidProtectionIntro.png

Case Study: (Anubis) BancaMarStealer

Cybercrime and financial fraud



BancaMarStealer



Follow

Anton Imail
@ImailAnton

1 Following **0** Followers

Tweets | Tweets & replies | Media | Likes

Anton Imail @ImailAnton · Aug 27

< zero
>MzA5MGMwOGFjNjI5MzkxZWRlOGQ2MzM0ODM3NDJiMTIwZDdkOGQ3Y
WZlZmVlZjUwMGY4Mjk3MWFiYTJlMTJjODI1ZjJmMzhlZDI5NTVmZjI3MmFm
Y2ExM2M4ZjZlYTk5ZjM=< /zero >

Anton Imail @ImailAnton · Aug 24

< zero
>MzA5MGMwOGFjNjI5MzkxZWRlOGQ2MzM0ODM3NDJiMTIwZDdkOGQ3Y
WZlZmVlZjUwMGY4Mjk3MWFiYTJlMTJjODI1ZjJmMzhlZDI5NTVmZjI3MmFm
Y2ExM2M4ZjZlYTk5ZjM=< /zero >

ZDNet

WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE NEWSLETTERS

MUST READ: Now this Android spyware poses as a privacy tool to trick you into downloading

These malicious Android apps will only strike when you move your smartphone

Apps containing the Anubis banking Trojan and an interesting motion sensor have been found in the Google Play store.

By Charlie Osborne for Zero Day | January 18, 2019 -- 11:52 GMT (03:52 PST) | Topic: Security

RSAConference2019

Apps will no longer be the Key Threat Vector

THE VERGE

APPLE | TECH | CYBERSECURITY

26

New WikiLeaks docs show how the CIA hacks iPhones and MacBooks

By Russell Brandom | @russellbrandom | Mar 23, 2017, 11:08am EDT

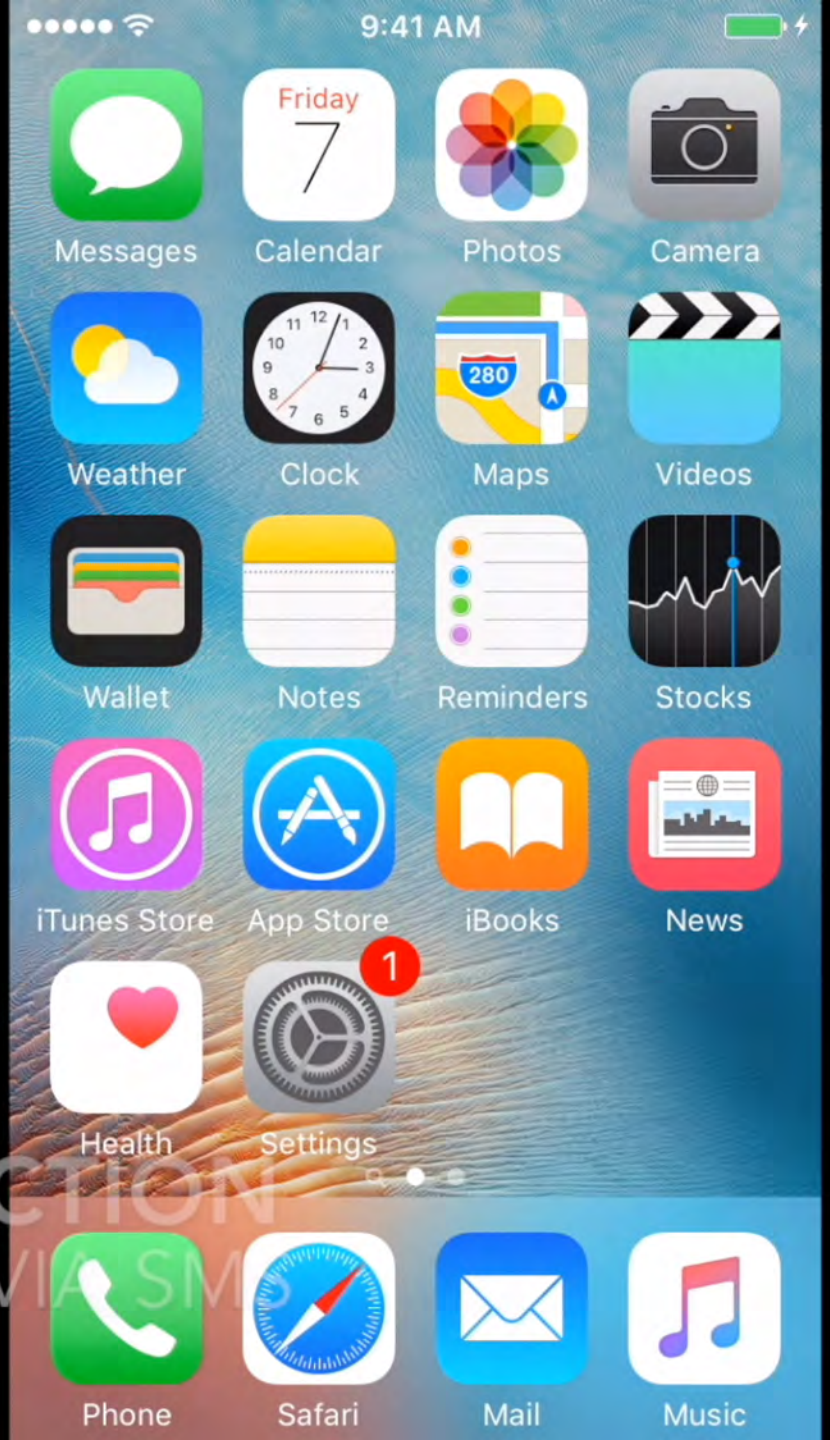
For years, the CIA has been developing tools for hacking into Apple products — and thanks to WikiLeaks, those tools are now public. Today, the group published a new set of documents dubbed "Dark Matter," part of the ongoing Vault 7 publication on CIA hacking tools. Today's documents focus specifically on Apple products, detailing the CIA's methods for breaking into MacBooks and iPhones.

Case Study: NSO Pegasus

Nation-state level mAPT as a Service


etisalat
2:41 PM
Messages (6)
InfoSMS
Details
Text Message
Today 1:44 PM
أسرار جديدة عن تعذيب إماراتيين في سجون الدولة : https://sms.webadv.co/9573305s/
TRANSLATION
New secrets about torture of Emiratis in state prisons [link]
iMessage
Send


11:50
Messages
Details
Text Message
Sr. Simon se acaba de accidentar [redacted] esta muy grave, espero venga, le paso los datos donde esta internada: http://bit.ly/2b2cdOM
TRANSLATION
Mr. Simon, [daughter's name] was just in an accident, she is in grave condition, I hope can you come, here is the where she is hospitalized: [link]
iMessage
Send

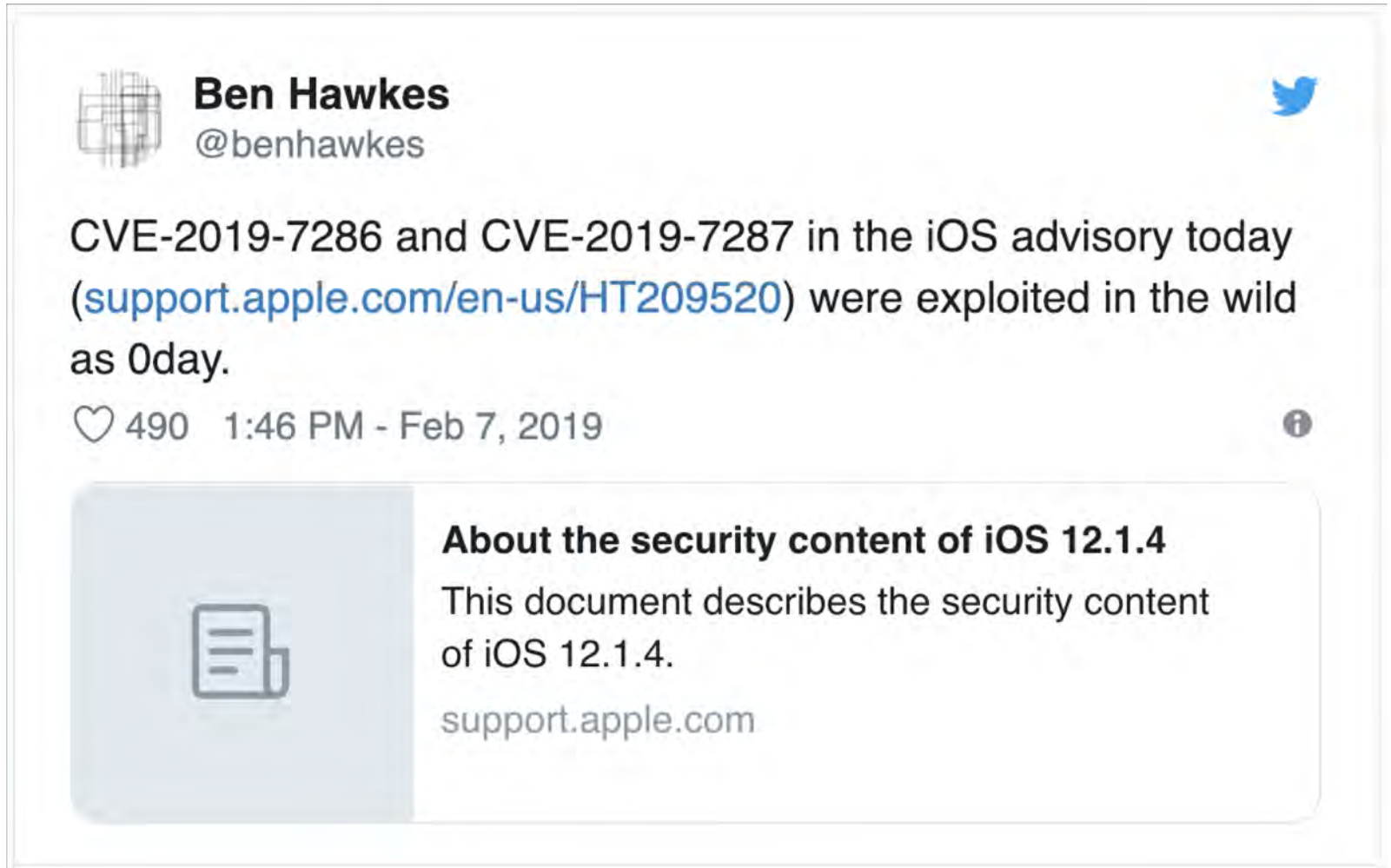


PEGASUS INFECTION

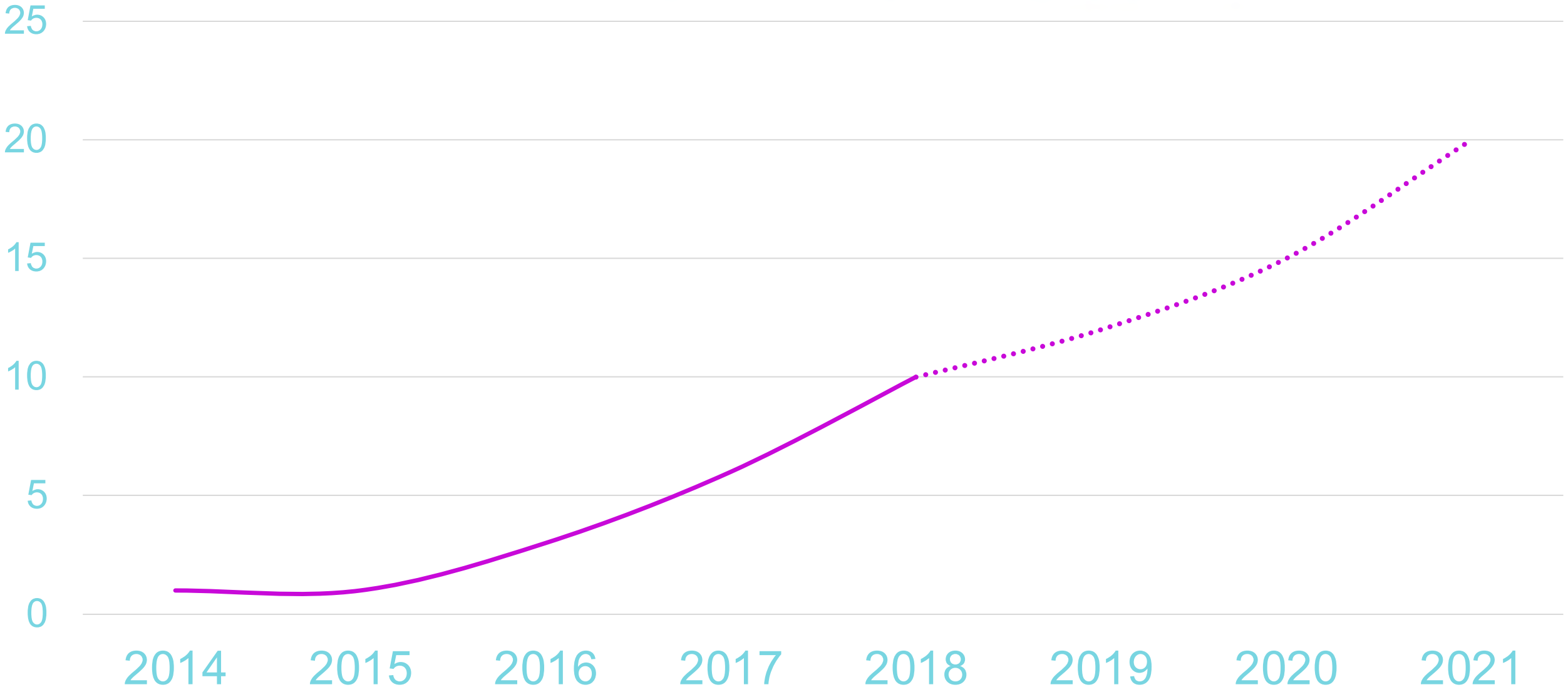
CLICKING A LINK VIA SMS

Lookout

Actor / Family	Reported	Overview
Pegasus (NSO Group)	August 2016	Device Compromise and Surveillance
Chrysaor (NSO Group)	April 2017	Device Compromise and Surveillance
ViperRAT	February 2017	App-based Surveillance
SonicSpy	August 2017	Targeted surveillanceware in Google Play
FrozenCell	October 2017	APT-C-23 Surveillanceware
JadeRAT	October 2017	Surveillanceware linked to Chinese Govt
Titan	November 2017	Surveillanceware linked to Tropic Trooper
SpyWaller v2	January 2018	Mobile APT surveillance
Dark Caracal/Pallas	January 2018	PC and Mobile surveillance
Desert Scorpion	April 2018	Targeted Surveillance on Google Play
Stealth Mango/Tangelo	May 2018	iOS and Android spyware kits


Ben Hawkes
@benhawkes
CVE-2019-7286 and CVE-2019-7287 in the iOS advisory today (support.apple.com/en-us/HT209520) were exploited in the wild as 0day.
490 1:46 PM - Feb 7, 2019
About the security content of iOS 12.1.4
This document describes the security content of iOS 12.1.4.
support.apple.com

Device Targeted mAPT



Apply What You Have Learned Today

- Next week you should:
  - Think about the various ways that an attack against your organization's mobile devices could create a breach?
- In the first three months following this presentation you should:
  - Examine your organization to determine how many mobile devices are accessing key resources
  - Reconsider how protecting your mobile endpoints fits as part of your current endpoint protection strategy
- Within six months you should:
  - Determine a strategy for protecting all of your modern OS devices in light of the direction of the mobile threat landscape.

RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MBS-T08

Questions?

Apurva Kumar
Staff Security Intelligence Engineer, Lookout
apurvakumar@lookout.com
Twitter: @abby_kcs

Michael Murray
Chief Security Officer, Lookout
mmurray@lookout.com
Twitter: @mmurray