The State of Phishing and Apps
• Founded in 2007
• Global presence with worldwide distribution and support
• Solutions for consumers, small-medium business, enterprise, and government
• We secure 500k businesses worldwide
• The only endpoint-to-cloud solution
• Including the largest organizations and highest levels of government

~200M MOBILE DEVICES
140M+ APPS ANALYZED
4.5M+

500+
PHISHING SITES/DAY
10K+
MALICIOUS APPS/DAY

MACHINE INTELLIGENCE

San Francisco
Toronto
Boston
Washington DC
London
Amsterdam
Dubai
Singapore
Japan
Sydney

MACHINE INTELLIGENCE

San Francisco
Toronto
Boston
Washington DC
London
Amsterdam
Dubai
Singapore
Japan
Sydney
Partnerships

Technology partners

Carrier Partners

Channel Partners
Leading market innovation

- Enterprise mobile security product
- Endpoint-to-cloud solution incl CASB and ZTNA
- Mobile phishing protection solution
- To support Zero Trust for Google and Microsoft
  - Integration with Microsoft Intune
  - Mobile security for Google BeyondCorp
- EDR built for mobile

Leveraging the largest dataset

- ~200M Devices
- 140M+ Apps
- 4.5M+ Domains per month

Identifying major threats

- Pegasus
- Chrysaor
- ViperRAT
- SonicSpy
- Frozen Cell
- JadeRAT
- Titan
- SpywallerV2
- Dark Caracal
- Desert Scorpion
- ViperRATv2
- Stealth Mango
- BancamarStealer
- DNC Phishing
- Monokle
- UN & NGO Phishing
- Canadian Bank Phishing
- SpyNote
- SilkBean
- Goontact
- Hornbill
- Canadian Bank Phishing
- SunBird
- JADE RAT
- Stealth Mango
- Corona Live 1.1

Discovering the most threat families

- Lookout - 1,975
- Trend - 31
- Kaspersky - 26
- Check Point - 21
- Symantec - 18
- ESET - 17
- Zimperium - 13
- Sophos - 11
- Zscaler - 7
- Google - 7
- Wandera - 6
- McAfee - 6
- Palo Alto - 6
- Dr.WEB - 3
- Microsoft - 1
- Crowdstrike - 0
Delivering integrated endpoint-to-cloud security

- USER
- ENDPOINT
- NETWORK
- CLOUD
- UEBA
- MEP
- EDR
- V&PM
- R&C
- PCP
- SWG
- ZTNA
- CASB
- DLP
Real World Exposure Rates
Q4 Global Mobile Exposure Rates

EMEA

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q4 2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>7.86%</td>
<td>8.83%</td>
</tr>
<tr>
<td>OS Vulnerabilities</td>
<td>1.70%</td>
<td>11.58%</td>
</tr>
<tr>
<td>App Threats</td>
<td>9.55%</td>
<td>4.80%</td>
</tr>
<tr>
<td>Device Risks</td>
<td>2.08%</td>
<td>4.09%</td>
</tr>
<tr>
<td>App Risk</td>
<td>0.02%</td>
<td>0.29%</td>
</tr>
<tr>
<td>Network Threats</td>
<td>0.19%</td>
<td>0.09%</td>
</tr>
<tr>
<td>Device/OS Threats</td>
<td>0.01%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

NORTH AMERICA

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q4 2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>4.93%</td>
<td>3.85%</td>
</tr>
<tr>
<td>OS Vulnerabilities</td>
<td>2.82%</td>
<td>1.19%</td>
</tr>
<tr>
<td>App Threats</td>
<td>19.84%</td>
<td>2.90%</td>
</tr>
<tr>
<td>Device Risks</td>
<td>7.82%</td>
<td>2.03%</td>
</tr>
<tr>
<td>App Risk</td>
<td>0.21%</td>
<td>0.09%</td>
</tr>
<tr>
<td>Network Threats</td>
<td>0.03%</td>
<td>0.05%</td>
</tr>
<tr>
<td>Device/OS Threats</td>
<td>0.01%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

ASIA PACIFIC

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q4 2020</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>7.88%</td>
<td>16.35%</td>
</tr>
<tr>
<td>OS Vulnerabilities</td>
<td>0.39%</td>
<td>1.91%</td>
</tr>
<tr>
<td>App Threats</td>
<td>9.47%</td>
<td>8.94%</td>
</tr>
<tr>
<td>Device Risks</td>
<td>2.65%</td>
<td>1.36%</td>
</tr>
<tr>
<td>App Risk</td>
<td>0.01%</td>
<td>0.06%</td>
</tr>
<tr>
<td>Network Threats</td>
<td>0.03%</td>
<td>0.11%</td>
</tr>
<tr>
<td>Device/OS Threats</td>
<td>0.03%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>
Mobile phishing in financial services
Challenge

A phishing attack can come from anywhere

- The design of mobile UI hides details typically visible on a computer that can help us identify a phishing attack.

- Traditional anti-phishing approaches on mobile devices quickly become privacy issues because they inspect message content.

- Not protecting against mobile phishing leaves a significant gap in an organization’s security posture.

Most Targeted Industries in 2020

- Telecommunications – 24.4%
- Legal - 22.5%
- Retail - 21.6%
- Financial Services - 14.7%
- Manufacturing - 12.1%
- Healthcare/Pharma - 8.5%
- Professional Services - 7.3%
- Government - 4.0%
Breaking down intent

In 2020, **14.7%** of financial services employees encountered a phishing link

- **46.9%** were built for credential harvesting
- **79.4%** were built for delivering malware

**85%** of mobile phishing attacks happen in apps outside of email

1. Verizon Mobile Security Index, February 2020
App threats and risky permissions
Exposure to malicious and risky apps

Quarterly Exposure Rates

- 2020 Q1
- 2020 Q2
- 2020 Q3
- 2020 Q4
Three key examples

Chrome for Android
- Triggered when Chrome renders malcrafted HTML content
- Sandbox escape via HTML allows access to Chrome’s capabilities without rooting
- MDM will not detect a successful exploit

Telegram for iOS
- 13 vulnerabilities were found in one version of Telegram
- A vulnerable library used for emoticons allowed for remote code execution
- Heavy impact to the enterprise because of the app’s popularity

SourMint SDK
- Popular iOS advertising SDK found to have extensive visibility into PII
- Heavy self-obfuscation occurs if the SDK detects any debugging or proxy tools on the device.
- Behavior modification helps it pass through App Store review process
App Analysis: Telegram for iOS

Risk Summary and Grade C

- Violates corporate policy
- Contains risky capabilities
- Uses unencrypted network communications
- May violate OWASP M3 Insecure Communication

Violations

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTI</td>
<td>Apps that access address book or microphone.</td>
</tr>
<tr>
<td>Design</td>
<td>Apps that access sms archive or location or address book.</td>
</tr>
<tr>
<td>High Threat</td>
<td>Apps that address book or location or microphone.</td>
</tr>
<tr>
<td>Location123</td>
<td>Apps that access location.</td>
</tr>
<tr>
<td>Toegang tot clipboard</td>
<td>Apps that access clipboard.</td>
</tr>
<tr>
<td>clipboard-test</td>
<td>Apps that access clipboard and are los.</td>
</tr>
<tr>
<td>hghgyc</td>
<td>Apps that access location.</td>
</tr>
</tbody>
</table>

Data Handling Security

**TRANSPORT SECURITY**

The app does not require certificate transparency on any communications.

This app can communicate insecurely for all network traffic, unless exceptions are listed below.

**STORAGE SECURITY**

Encrypted files may be accessed after the device has been unlocked for the first time.

Capabilities

<table>
<thead>
<tr>
<th>TYPE</th>
<th>NAME</th>
<th>DETAILS</th>
<th>RISK EXPOSURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Access</td>
<td>Accesses camera</td>
<td>–</td>
<td>Critical</td>
</tr>
<tr>
<td>Data Access</td>
<td>Accesses the clipboard</td>
<td>–</td>
<td>Critical</td>
</tr>
<tr>
<td>Data Access</td>
<td>Records audio</td>
<td>–</td>
<td>Critical</td>
</tr>
<tr>
<td>Data Access</td>
<td>Reads contacts</td>
<td>–</td>
<td>Elevated</td>
</tr>
<tr>
<td>Data Access</td>
<td>Reads device sensor data</td>
<td>–</td>
<td>Elevated</td>
</tr>
<tr>
<td>Data Access</td>
<td>Reads location</td>
<td>–</td>
<td>Elevated</td>
</tr>
<tr>
<td>App Lifecycle</td>
<td>Accesses Private API</td>
<td>–</td>
<td>Elevated</td>
</tr>
<tr>
<td>Data Access</td>
<td>Uses local storage</td>
<td>–</td>
<td>Normal</td>
</tr>
<tr>
<td>Inter-App Interaction</td>
<td>Registers URI handler</td>
<td>Scheme:</td>
<td>Normal</td>
</tr>
</tbody>
</table>

Network
Bringing it all together: BancamarStealer

- Delivered by SMS and prompts target to download a customized (malicious) app.
- The malware can harvest credentials, implement screen overlays, send the user to other malicious sites, retrieve all SMS, and take control of the device remotely.
- Primary use case is trojanizing banking apps, but it’s fully customizable.
- Samples have been analyzed that overlay Amazon, Facebook, Skype, Twitter, Uber, and WhatsApp.
- First announced by Lookout researchers in 2018. In the last 3 years, the number of observed samples has grown from 7,700 to over 74,000.
Where do we go from here?
What life has taught us

Cloud-based security solutions secure your employees where on-prem or on-device solutions fall short.

Secure all devices from endpoint to cloud by implementing mobile security, cloud access security brokerage (CASB), and zero trust network architecture (ZTNA) across devices with one solution.

Use the best data you can. This ensures that your employees are protected from the latest known and unknown threats.

Build access policies based on the risk profile of the device. This includes vulnerable app versions that need to be updated, out of date OSs, risky network connections, and malicious content being present.

Proactively hunt for threats by leveraging app, device, phishing, and network threat data.
Thank you!