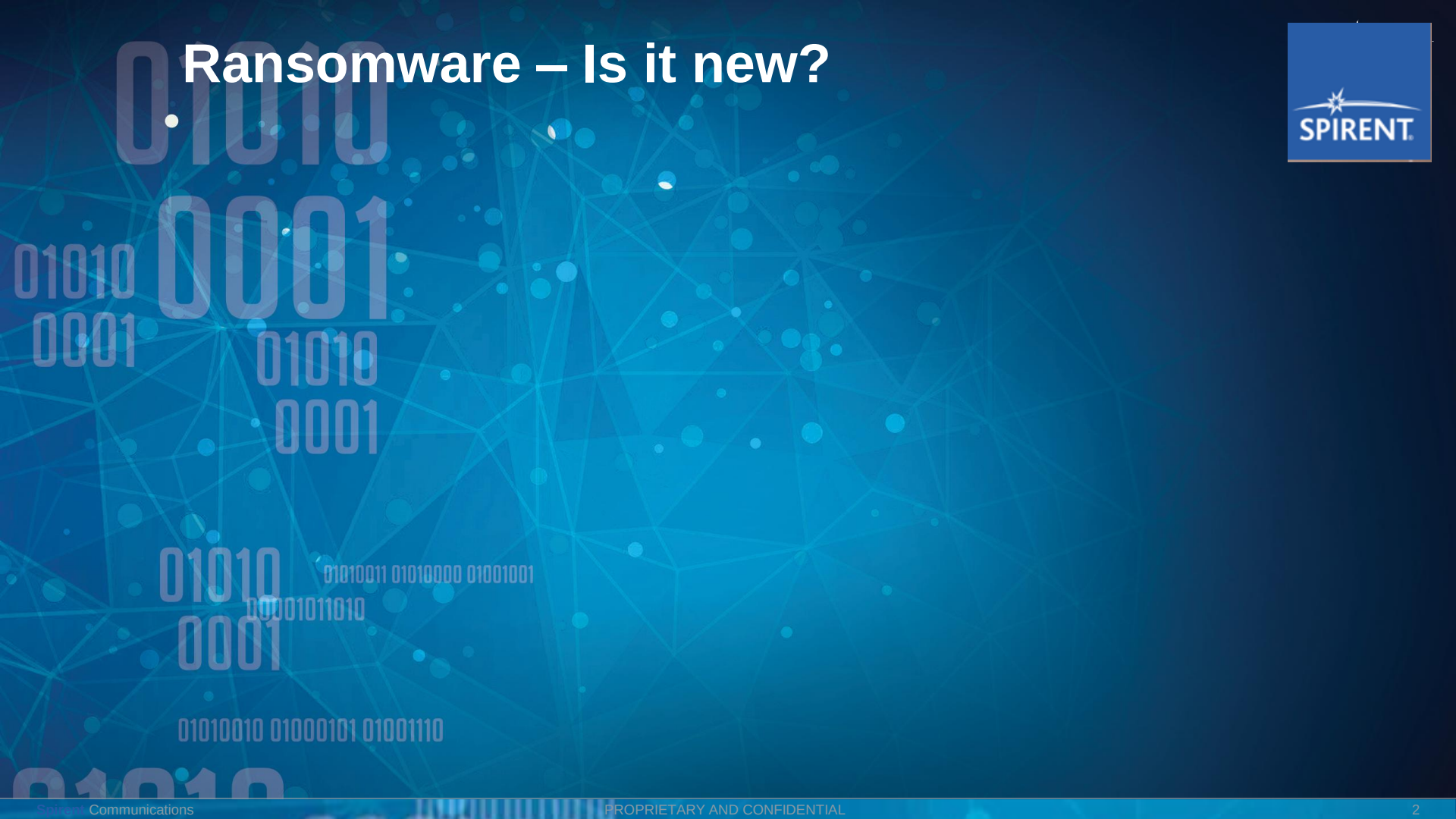
Spirent Security

Realistic Preemptive Intelligence

Hardening Defenses Against Tomorrow's Attacks

Ransomware – Is it new?



Ransomware – Is it new?

- First in 1989, PC CyBOrg
- Grew up prominent in 2005, CryZIP, Archiveus popular ones.

Application Security / Cyber Security ?

Application Security?

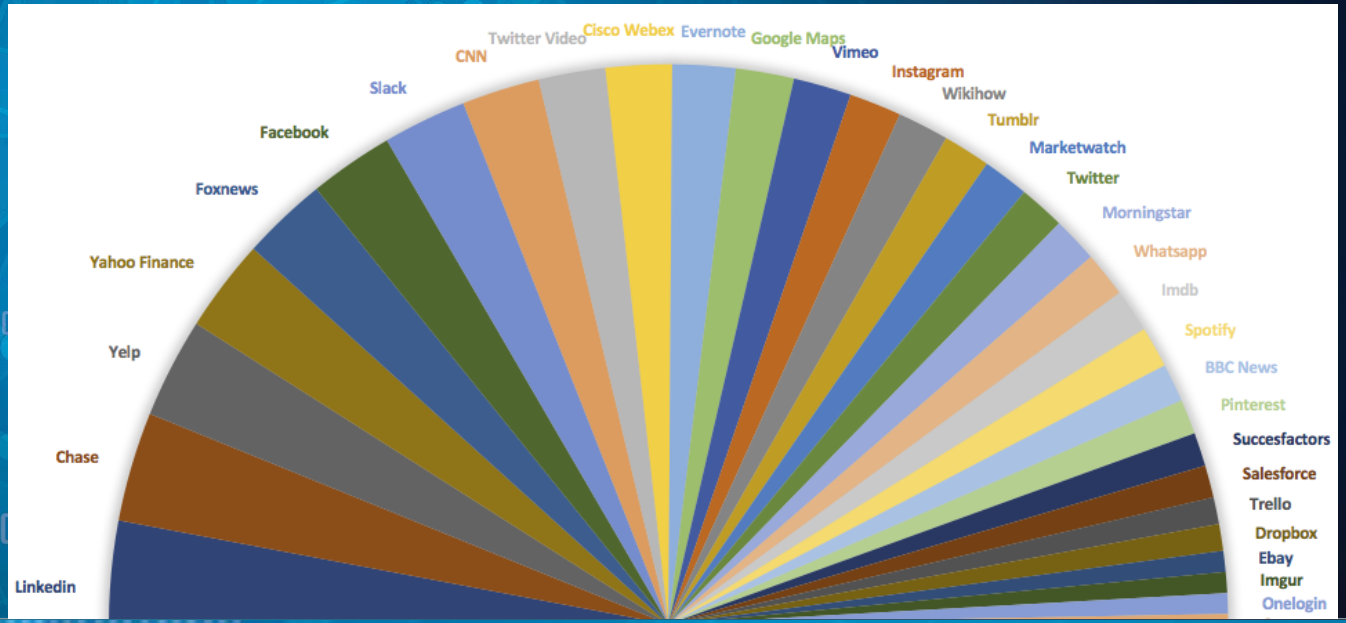
- Insider intrusion / HIPS – 60% attacks
- Attack surface / landscape growing exponentially in Cyber Security
- App – Mobile App, web App, DB App, Team collaboration,etc

Application Security?

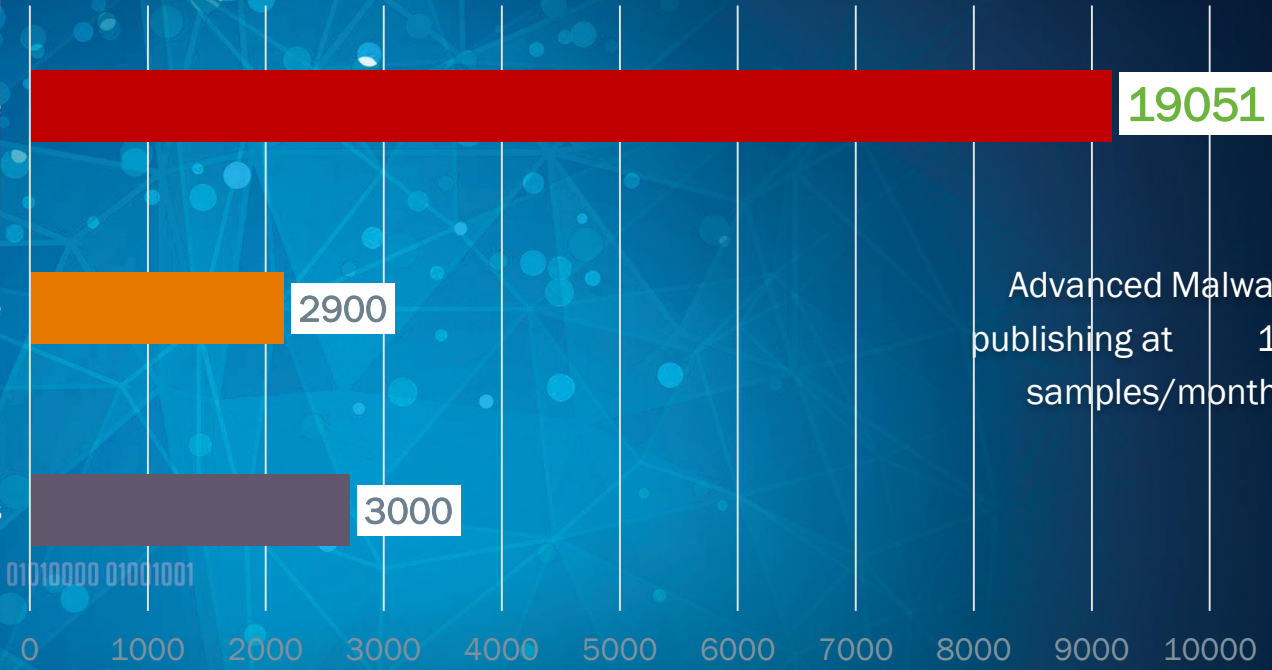
- Right mix to hit DPI / Network Endpoints
- Attacks / Malwares – platform centric attacks
- Device centric attacks / apps / malwares

First NetSecOPEN Program – Sec Traffic Mix

- Modern Enterprise Perimeter NGFW Traffic Mix for Firewall, IPS and NGFW tests
- Blend of ~70% HTTPS and ~30% HTTP
- ~10K unique URLs
- ~1000 unique FQDNs
- ~400 unique Certs
- ~80 Apps



TestCloud – Current Content Numbers



Advanced Malware publishing at 1500 samples/month!

Next Generation Security & Performance Testing

- Validate security coverage from enterprise to carrier-grade network capacity

- **Firewalls (FW)**
- **Intrusion Prevention (IPS)**
- **Application Delivery (ADC)**
- **Advanced Threat Protection (ATP)**
- **Secure Web Gateway (SWG)**
- **Secure Mail Gateway**
- **Unified Threat Management (UTM)**
- **Web Application Firewall (WAF)**
- **Next Generation Firewalls (NGFW)**
- **Next Generation Intrusion Prevention (NGIPS)**
- **Distributed Denial-of-Service Protection (DDoS)**
- **Software Defined WAN (SD-WAN)**
- **Data Loss Prevention (DLP)**
- **Enterprise Routers**
- **Secure Routers**
- **Video Gateways**

cybeflood

Security and Applications

Security and Performance Testing for App-Aware Solutions

Extending Your Cyber Security Team to Identify and Mitigate Risk

SecurityLabs Overview

Team of experienced security speciaalists providing complete range of security services

Managed Vulnerability Scanning
&
Penetration Testing

- **Network, Wireless & SCADA**
- **Web and Mobile Applications**
- **Devices (SmartHome, Network Devices, Banking, Automotive)**

Network - Systems, Services, Firewall, IDS, IPS etc.

Application - Authentication, Authorization, Input Validation

Device Hardware - Unauthorized Access, Encryption, Data security

Mobile - Client Data Storage, Data Transport, API

Cloud - Backend Server, Authorization, Update security

Spirent **SecurityLabs** PenTesting Methodology

Web Application

- Input Validation
  - XSS
  - SQL Injection
  - BufferOverflow
  - Phishing
  - CSRF
  - Cookie Security
- Authentication
- Authorization Boundary
- Encryption usage
- Lockout
- Brute force
- SSL/TLS Weakness
- Policy Compliance
- Static Code Analysis

Mobile Application

- Dynamic Analysis
- Binary Code Analysis
- Device End Security
  - Sensitive information stored in cache
  - Unencrypted Data Storage
  - Unrestricted File Upload
  - Files inspection
  - Excess Permissions and Privileges
  - Device Lockout policy
- Authentication/ Authorization
- Encryption usage

Network & Wireless

- Insecure Server Configuration
- Default System Passwords
- Unpatched systems
- Known Vulnerabilities & Exploits
- Insecure Firewall Configuration
- Information Leakage
- Improper Error Handling
- Data Exfiltration
- Evil Twin
- Weak cryptographic keys
- Vulnerable Ciphers and Protocols
- User Demonization
- Jamming

Embedded Device

- Device Firmware Analysis
- Binary Code Analysis
- Webservices review
- Authentication bypass
- Authorization logic
- Encryption usage
- Underlying Software & application evaluation
- Unencrypted Communication
- Spoofing
- Fuzzing

securitylabs
spirent.com

THANK YOU !!


01010
0001
01010
0001
01010
0001
01010
0001
01010011 01010000 01001001
01010011010
01010010 01000101 01001110