BitLyft | CYBERSECURITY

Jason Miller | CEO

Jason.miller@bitlyft.com
LinkedIn: /jasonmillerbitlyft

www.bitlyft.com
CYBER ATTACKS: THE INVISIBLE THREAT
Think cyberattacks are not an issue?

www.bitlyft.com
ATLANTA SPENT $2.6M TO RECOVER FROM A $52,000 RANSOMWARE SCARE

Baltimore becomes the third U.S. city in a week to be hacked

By Lezlie White | May 29, 2018

Ransomware attack against California provider breaches data of 85,000 patients

By Jessica Davis | April 26, 2018 | 02:27 PM

Ransomware, Privacy, User Data, Facebook, Hacked. Those words and been all over the news in the past couple of weeks. Just last week, the Atlanta’s computer network was hacked and those responsible demand in ransomware to allow the city to regain its systems. Computer repair William Allen, talks with WEAK’s Lezlie White about how not only to protect computers, but your privacy on social media as well.

The City of Leeds, Alabama, a small community just outside of Birmingham, was hacked and the hackers demanded and were paid $12,000. In Baltimore, officials say the 911 dispatch system was hacked over the weekend, causing a temporary shutdown of automated dispatching.
National Cyber Awareness System:

**TA18-106A: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices**

*04/16/2018 01:25 PM EDT*

Original release date: April 16, 2018

**Systems Affected**

- Generic Routing Encapsulation (GRE) Enabled Devices
- Cisco Smart Install (SMI) Enabled Devices
- Simple Network Management Protocol (SNMP) Enabled Network Devices

**Overview**

This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the United Kingdom’s National Cyber Security Centre (NCSC). This Technical Alert discusses malicious activity targeting network infrastructure devices.
Common visible vectors for an attacker

- **Humans!**
  - We make mistakes
- **Hardware devices.**
  - Endpoints
  - Servers
  - Firewalls
  - Switches
  - Smart Devices (IoT)
- **Exploited configurations**
  - Insecure software
- **Malicious software**
  - Causes confusion
  - Looks exactly like what your used to seeing
Email | Web Browser
DNS | Fileless Malware
Insider Threat
Invisible Threats

- Compromised accounts go un-noticed
  - Office 365 accounts being used, un-noticed to system administrators.
- VOIP Phone systems
  - SIP calls to foreign countries
- Your company’s logo on a vendor website or other marketing collateral.
Dropbox
Network traffic from machine going out to China and Russia.
Mature SIEM is well integrated across the entire IT landscape
Machine Data Intelligence Fabric

Data Collection

Data Generation

Search Analytics

Machine Analytics

Machine Data Intelligence (MDI) Fabric

- Uniform Data Classification
- Uniform Data Structure
- Time Normalization
- Risk Score
- User Persona
- Host Persona
- Geolocation
- Flow Direction
- ...more

Benefits

- Serves as IT environment abstraction layer
- Enables generic scenario representation
- Allows for high-efficacy packaged analytics modules

LogRhythm Network Monitor
LogRhythm System Monitor

www.bitlyft.com
Bitlyft’s Unified Approach

1st
SIEM

- Foundational
- Monitoring
- Detection
- Alarms
- Log Collection
- Compliance Reporting
- SIEM notifies SOAR

2nd
SOC

- Security Analysts
- Augmenting existing IT Team
- On-going Communication between BitLyft Security Analysts and Client
- Developers building automation

3rd
SOAR

- Security Orchestration Automated Response
- Within minutes neutralize threats
- Reports the threat to “Relay”

4th
RELAY

- Identifies similar clients
- Uses SOAR to take preventive action on those similar clients

www.bitlyft.com
Needs

You have to be proactive, have some type of UEBA that looks at user behavior and how they are interacting with your network, as well as a centralized location for log data so that you have real visibility into your network.

Without visibility you have no real way of knowing whether you are under attack until it is too late.
In 2017 - One in 131 emails sent were malicious.

Build advanced malware defenses into and across your entire network and endpoints.

You’re responsible for your Cloud... AWS, Azure and Google are not responsible for your data.

**Indicators-Warnings of Attack**: What activities, events, conditions, or behaviors could serve as indicators that an attack is imminent, in progress, or has occurred?

**Obfuscation**: What techniques are typically used to disguise the fact that an attack is imminent, in progress, or has occurred?

You can’t change, what you aren’t measuring!
Jason Miller | CEO

Jason.miller@bitlyft.com
LinkedIn: /jasonmillerbitlyft

www.bitlyft.com