THE GREATEST GIFT
DIRECTOR OF CYBER DEFENSE, CENTURYLINK

BILL SWEARINGEN

Cyber Incident Response Team
Cybersecurity Vulnerability Services
Corporate Forensics
Cybersecurity Infrastructure and Architecture
Internet Security Services
Defenders have to get security right every time

An attacker only has to get it right once.
**The Greatest Gift**

---

**Proactive**

**Detection Efficiency**

**Reconnaissance**
- Gather email, website and personnel info

**Weaponization**
- Create exploit payload bundle

**Delivery**
- Deliver weaponized bundle via email, web, USB, network, etc.

**Exploitation**
- Exploit a vulnerability to execute code on the victim’s system.

**Installation**
- Install malware on the victim’s system.

**Command and Control**
- Establish a communications channel for remote commands

**Action on Objectives**
- Accomplish original goals inside victim network.

---

**Compromise**

**Software Patching**
- Port, Protocol, & State Analysis
- Default deny policy
- User Awareness
- Threat Intelligence Feed

**Host Protections**
- Anti-Virus
- Host Firewall
- Host Intrusion Detection

**Limited administrator rights**

**Email Gateway**
- 98.9% of all inbound email is filtered (spam or phishing)

**Network Visibility**
- Netflow and Full Packet Capture

**Email**
- Two Factor Remote Access

**CTL Threat Intelligence Center**

**Data Loss Prevention (DLP)**

**Host Forensics**

**Security Information and Event Management (SIEM)**

**System Backup**

---

**Proactive**

**Detection Efficiency**

**Reconnaissance**
- Gather email, website and personnel info

**Weaponization**
- Create exploit payload bundle

**Delivery**
- Deliver weaponized bundle via email, web, USB, network, etc.

**Exploitation**
- Exploit a vulnerability to execute code on the victim’s system.

**Installation**
- Install malware on the victim’s system.

**Command and Control**
- Establish a communications channel for remote commands

**Action on Objectives**
- Accomplish original goals inside victim network.

---

**Compromise**

**Software Patching**
- Port, Protocol, & State Analysis
- Default deny policy
- User Awareness
- Threat Intelligence Feed

**Host Protections**
- Anti-Virus
- Host Firewall
- Host Intrusion Detection

**Limited administrator rights**

**Email Gateway**
- 98.9% of all inbound email is filtered (spam or phishing)

**Network Visibility**
- Netflow and Full Packet Capture

**Email**
- Two Factor Remote Access

**CTL Threat Intelligence Center**

**Data Loss Prevention (DLP)**

**Host Forensics**

**Security Information and Event Management (SIEM)**

**System Backup**

---

**Detection**

**Comromise**

**DETECTION**

**COMPROMISE**

**Email Gateway**
- 98.9% of all inbound email is filtered (spam or phishing)

**Software Patching**
- Port, Protocol, & State Analysis
- Default deny policy
- User Awareness
- Threat Intelligence Feed

**Host Protections**
- Anti-Virus
- Host Firewall
- Host Intrusion Detection

**Limited administrator rights**

**Email Gateway**
- Two Factor Remote Access

**Software Patching**
- Intrusion Detection Systems

**Host Protections**
- Advanced Network Protection

**Limited administrator rights**

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.

**Software Patching**
- Thousands of these events per day.

**Host Protections**
- Thousands of these events per day.

**Email Gateway**
- Thousands of these events per day.
THE ATTACKER
Specific plugins are targeted when critical vulnerabilities and exploits are published.
ATTACK INFRASTRUCTURE

- Reconnaissance
- Weaponization

Bullet Proof Hosting

DELIVERY

COMMAND AND CONTROL

VICTIM INFRASTRUCTURE
ATTACK INFRASTRUCTURE

ATTACKER

Bullet Proof Hosting

DELIVERY

COMMAND AND CONTROL

EXPLOITATION INSTALLATION

ACTION ON OBJECTIVES

VICTIM INFRASTRUCTURE

Reconnaissance | Weaponization | Delivery | Exploitation | Installation | Command and Control | Action on Objectives
Will the red team please stand up.
The Greatest Gift

Cyber Kill Chain

Reconnaissance
- Gather email, website and personnel info

Weaponization
- Create exploit payload bundle

Delivery
- Deliver weaponized bundle via email, web, USB, network, etc.

Exploitation
- Exploit a vulnerability to execute code on the victim’s system

Installation
- Install malware on the victim’s system

Command and Control
- Establish a communications channel for remote commands

Action on Objectives
- Accomplish original goals inside victim network

Detection Efficiency
- Port, Protocol, & State Analysis
- Default deny policy
- User Awareness
- Threat Intelligence Feed

Reconnaissance & Weaponization
- Email Gateway
  - 98.9% of all inbound email is filtered (spam or phishing)
- Two Factor Remote Access

Detonation
- Millions of these events per day

Software Patching
- Source Code Analysis
- Intrusion Detection Systems
- Advanced Network Protection

Detection
- Limited administrator rights
- Endpoint visibility

Exploitation & Weaponization
- Thousands of these events per day

Host Protections
- • Anti-Virus
- • Host Firewall
- • Host Intrusion Detection

Installation & Command and Control
- Hundreds of these events per day

Host Forensics
- Security Information and Event Management (SIEM)
- System Backup

Operation & Control
- Hundreds of these events per month

Action on Objectives & Detonation
- A few of these per year

The Greatest Gift
OBJECTIVE COMPLETE

ON THE LAST DAY OF THE ENGAGEMENT
MAKE ATTACKING EXPENSIVE
MALWARE IS THE GREATEST GIFT AN ATTACKER CAN GIVE
The phishing email attempted to hide in plain site by intermixing legitimate Amazon links.

**Malicious Link #1:** hxxp://www.aquadrift.sk/wp-content/themes/yoo_glass_wp/1.php

**Malicious Link #2:** hxxp://cartorialbuquerque.com.br/images/1.php

**Malicious Link #3:** hxxp://capdienphuthai.com/wp-content/themes/RaoThue/1.php

**Malicious Link #4:** hxxp://hydroac.info/wp-content/themes/twentyfourteen/1.php

**Malicious Link #5:** hxxp://urduacademyjeddah.com/wp-content/themes/novado/1.php

 Samples hosted in countries all over the world including Russia, Thailand, Brazil, Solvak Republic, and United States.
hxxp://www.aquadrift.sk/wp-content/themes/yoo_glass_wp/1.php
hxxp://cartorioalbuquerque.com.br/images/1.php
hxxp://capdienphuthai.com/wp-content/themes/RaoThue/1.php
hxxp://hydroac.info/wp-content/themes/twentyfourteen/1.php
hxxp://urduacademyjeddah.com/wpcontent/themes/inovado/1.php
INDICATOR OF COMPROMISE

http://www.aquadrift.sk/wp-content/themes/yoo_glass_wp/1.php
http://cartorioalbuquerque.com.br/images/1.php
http://capdienphuthai.com/wp-content/themes/RaoThue/1.php
http://hydroac.info/wp-content/themes/twentyfourteen/1.php
http://urduacademyjeddah.com/wpcontent/themes/inovado/1.php
INDICATOR OF COMPROMISE

hxxp://www.aquadrift.sk/wp-content/themes/yoo_glass_wp/1.php
hxxp://cartorioalbuquerque.com.br/images/1.php
hxxp://capdienphuthai.com/wp-content/themes/RaoThue/1.php
hxxp://hydroac.info/wp-content/themes/twentyfourteen/1.php
hxxp://urduacademyjeddah.com/wpcontent/themes/inovado/1.php

THREAT INTELLIGENCE
WHAT IS THREAT INTELLIGENCE

Users Targeted
Sending Address
Subject Line
Attachment Hash

IP ADDRESS
DOMAIN NAME
USER AGENT
REGULAR EXPRESSION

FILE HASH
PROCESS NAME
USER CREDENTIALS
Workspace Tools

Local Sandbox
- Cuckoo Sandbox: www.cuckoosandbox.org
- Remnux: remnux.org
- Malheur: mlsec.org/malheur

Cloud Sandbox
- Malwr: malwr.com
- Payload Security: hybrid-analysis.com
- Mastiff-Online: mastiff-online.korelogic.com
- ThreatExpert: threatexpert.com
- Anubis: anubis.iseclab.org
- VirusTotal: virustotal.com

Office and PDF Scanners – Local
- OfficeMalScanner: reconstructorer.org
- OffVis: aldeid.com/wiki/OffVis
- PDFxRay_Lite: github.com/9b/pdfxray_lite

Office and PDF Scanners – Cloud
- XecScan: scan.xecure-lab.com
- Malware Tracker: malwaretracker.com

Sandbox Behavioral Tools
- Regshot: sourceforge.net/projects/regshot
- MAP: github.com/dzzie/MAP
- Sysinternals: live.sysinternals.com

Virtual Machine
- Virtualbox: virtualbox.org/wiki/Downloads
- Vmware: vmware.com/products/player

Reverse Engineering
- IDA Pro: hex-rays.com/products/ida/
- OllyDbg: ollydbg.de/download.htm

Threat Intelligence
- CRITS: crits.github.io
- SOLTRA: soltra.com
Attackers only have to be wrong once