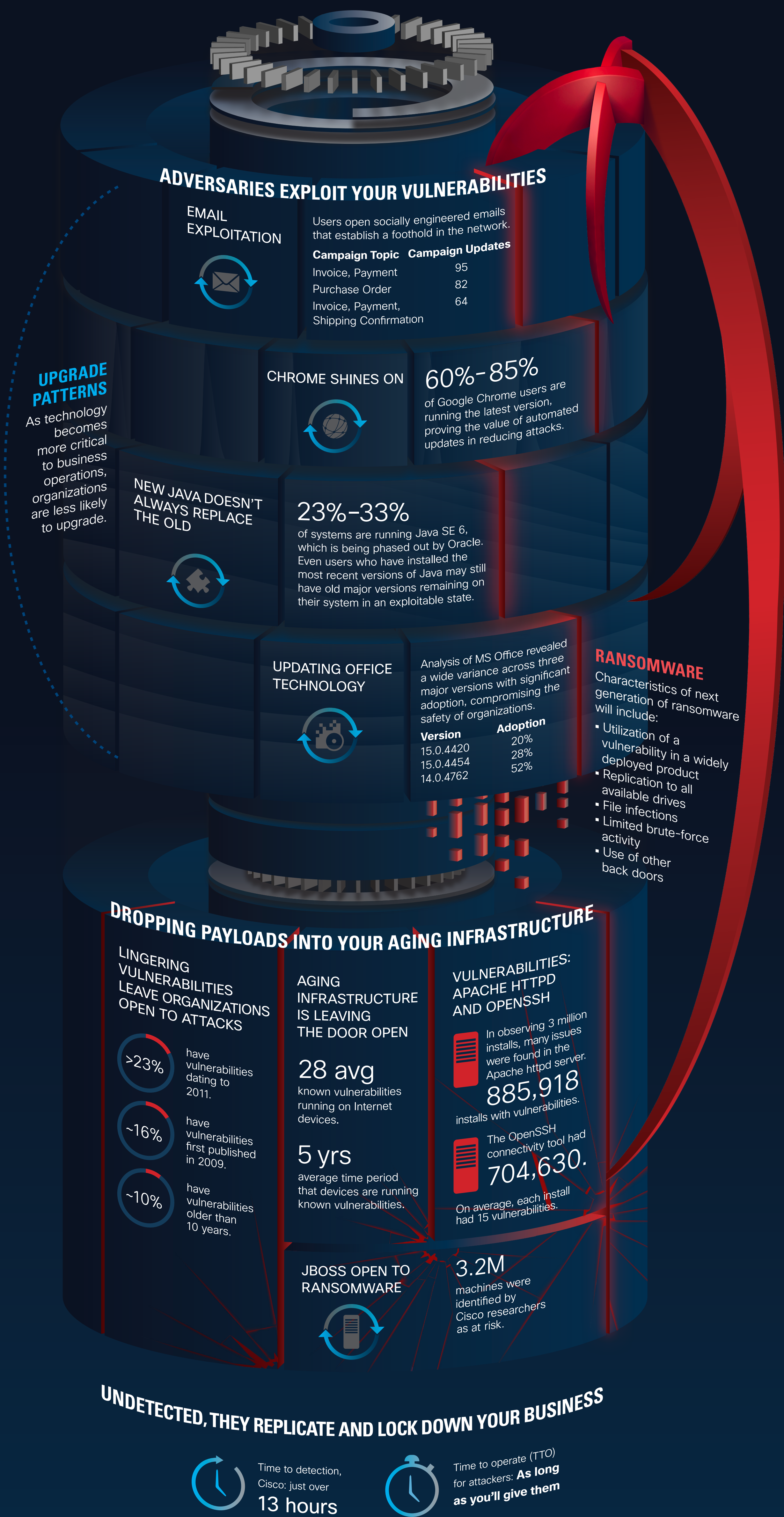# Poor Network Hygiene Attracts Malicious Activity.

Digitally dependent systems now run every aspect of business. A highly vulnerable hodgepodge of web browsers, applications, and infrastructure has created a fragile foundation. And while defenders are constantly innovating, the next breach could set it up for collapse.

ADVERSARIES EXPLOIT YOUR VULNERABILITIES

EMAIL EXPLOITATION

Users open socially engineered emails that establish a foothold in the network.

Campaign Topic	Campaign Updates
Invoice, Payment	95
Purchase Order	82
Invoice, Payment, Shipping Confirmation	64

UPGRADE PATTERNS

As technology becomes more critical to business operations, organizations are less likely to upgrade.

CHROME SHINES ON

60%–85% of Google Chrome users are running the latest version, proving the value of automated updates in reducing attacks.

NEW JAVA DOESN'T ALWAYS REPLACE THE OLD

23%–33% of systems are running Java SE 6, which is being phased out by Oracle. Even users who have installed the most recent versions of Java may still have old major versions remaining on their system in an exploitable state.

UPDATING OFFICE TECHNOLOGY

Analysis of MS Office revealed a wide variance across three major versions with significant adoption, compromising the safety of organizations.

Version	Adoption
15.0.4420	20%
15.0.4454	28%
14.0.4762	52%

RANSOMWARE

Characteristics of next generation of ransomware will include:

- Utilization of a vulnerability in a widely deployed product
- Replication to all available drives
- File infections
- Limited brute-force activity
- Use of other back doors

DROPPING PAYLOADS INTO YOUR AGING INFRASTRUCTURE

LINGERING VULNERABILITIES LEAVE ORGANIZATIONS OPEN TO ATTACKS

>23% have vulnerabilities dating to 2011.

~16% have vulnerabilities first published in 2009.

~10% have vulnerabilities older than 10 years.

AGING INFRASTRUCTURE IS LEAVING THE DOOR OPEN

28 avg known vulnerabilities running on Internet devices.

5 yrs average time period that devices are running known vulnerabilities.

VULNERABILITIES: APACHE HTTPD AND OPENSSH

In observing 3 million installs, many issues were found in the Apache httpd server.

885,918 installs with vulnerabilities.

The OpenSSH connectivity tool had **704,630.**

On average, each install had 15 vulnerabilities.

JBOSS OPEN TO RANSOMWARE

3.2M machines were identified by Cisco researchers as at risk.

UNDETECTED, THEY REPLICATE AND LOCK DOWN YOUR BUSINESS

Time to detection, Cisco: just over **13 hours**

Time to operate (TTO) for attackers: **As long as you'll give them**

Poorly protected devices and software open up operational space to adversaries. It's up to you to eliminate it. Priority must be placed on reducing unconstrained operational space and making adversary presence known.

To learn more about how you can close your security gaps, download the Cisco 2016 Midyear Cybersecurity Report at

www.cisco.com/go/mcr2016

CISCO