Ransomware - how to stop it

Ransomware has affected all types of public and private organizations including US state and Local government, healthcare providers, large international enterprises and even managed IT service providers. Will this scourge stop anytime soon? Probably not. As Willie Sutton is claimed to have said when asked why he robs banks, “That’s where the money is”. As long as attackers can relatively easily perform successful ransomware attacks and get paid, these attacks will likely continue.

The important thing to know is that these attacks can almost all be prevented. Not by putting the perpetrators in jail, like Willie Sutton, but by implementing cyber defense best practices, such as those recommended by the Center for Internet Security (CIS).[1] Belarc’s products can help orga-

[1] Center for Internet Security (CIS) Basic Controls. We like the CIS controls because they are based on lessons learned from actual attacks and breaches and are created by people from multiple industries and government, including the NSA and DHS, who have deep knowledge of all aspects of cyber security.

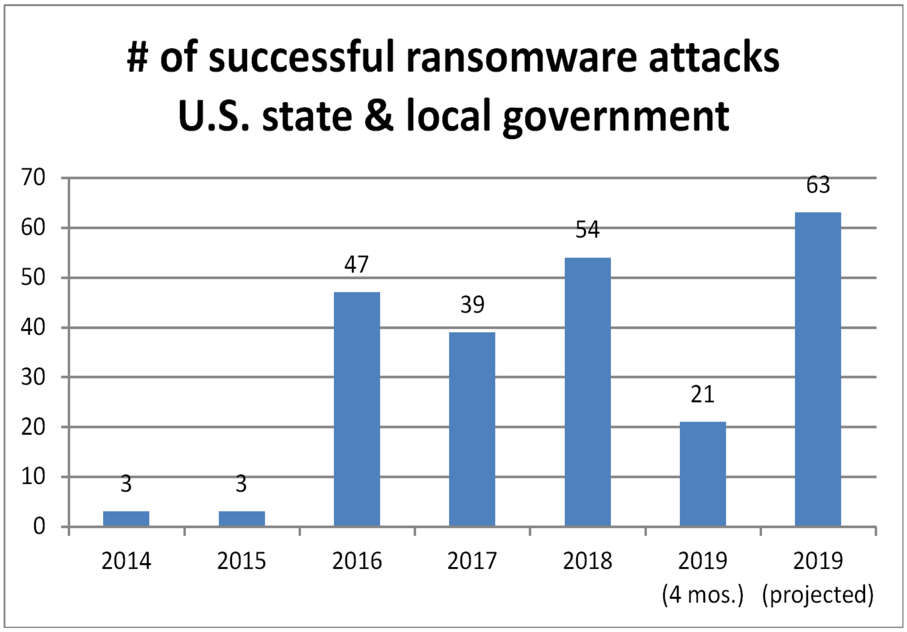
nizations of any size implement the CIS Top 5 controls in an automated and cost effective way.[2]

Impact

The impact that ransomware has had on organizations of all sizes over just the past few years is astonishing. Here are a few examples:

U.S. state and local government

At least 170 U.S. state and local organizations have been successfully attacked by ransomware since 2013, with the most occurring in the past few years. See chart below.[3]



Some of these attacks have been quite expensive in time and money and the negative impacts on government operations and services to its citizens. Well published examples include attacks on the following:

[2] Our Oakland County, MI customer has stated that Belarc's system helped them prevent successful ransomware attacks over the past few years.

[3] "Early Findings: Review of State and Local Government Ransomware Attacks", Recorded Future, April 2019

- Atlanta, GA, where the ransomware attack affected almost all of the city's agencies and cost the city an estimated $17 million in direct costs.[4]

- Baltimore, MD, where the city's payment and email services were off-line for two months.

- Riviera Beach, FL, where emergency response systems and email were down and the town decided to pay a ransom of $600,000.[5]

As cities and state agencies continue to offer more digital services, the impact of a successful ransomware attack will become ever more devastating to them and their citizens.

Healthcare

Healthcare has also been a target for ransomware maybe because of the need to bring critical systems back on-line quickly. Some examples of healthcare organizations being negatively impacted by ransomware are:

- The U.K. National Health Service (NHS), which was impacted by the 2017 WannaCry outbreak and brought hundreds of NHS facilities to a standstill for several days.

- Erie County Medical Center, NY, which lost access to thousands of its computers for many weeks and the recovery process cost $10 million.

- Reckitt Benckiser, the owner of brands such as Air Wick, Calgon, Dettol, Durex and many others, announced that the NotPetya ransomware cost it $140 million.[6]

World-wide enterprises

Even large world-wide enterprises are not immune to ransomware breaches. Some notable examples are:

- Maersk, the world's largest container ship and supply vessel operator, suffered $300 million of business operations losses.[7]

[4] U.S. CITIES ARE UNDER ATTACK FROM RANSOMWARE — AND IT'S GOING TO GET MUCH WORSE, Vice News, June 17, 2019

[5] Florida town pays $600,000 virus ransom, BBC Technology, 21 June 2019

[6] Understanding the true, hidden costs of ransomware attacks on the business, Acronis.

- Renault and Nissan were forced to idle plants in France, Slovenia, Romania after the WannaCry epidemic.
- Norsk Hydro, one of the largest aluminium producers, was successfully attacked by ransomware that impacted both its IT and OT (operational technology) systems, affected 22,000 computers, and has taken months to recover at a cost of at least $57 million in lost revenue.[8]
- Wloters Kluwer was impacted by ransomware in early May 2019 and it's CCH unit which provides software and services for accounting, tax and audit was off-line for days. The company has not disclosed the costs of this disruption.[9]

Managed Service Providers (MSPs)

MSPs, who offer IT services to their customers, are being compromised so that the attackers can plant ransomware on their customers' computers. MSPs have the ability to update software on their customers' machines and apparently the attackers are compromising these management systems to plant ransomware on the MSPs customers' systems. This is a pretty scary scenario, because even if the end user is doing all the rights things to prevent a ransomware attack, if their MSP's system is compromised they can be also.[10]

The How and Why of Ransomware

We've already explained why ransomware happens. As in Willie Sutton's quote, it's where the money is. Ransomware is about earning money for the attackers. It is not done for espionage or data exfiltration purposes. Studies of Bitcoin transactions show that ransomware payments made to attackers have been at least $100 million (2013-2017)[11] and growing.

[7] Understanding the true, hidden costs of ransomware attacks on the business, Acronis

[8] How a ransomware attack cost one firm £45m, BBC News, 25 June 2019

[9] Information Services Giant Wolters Kluwer Hit by Malware Attack, SecurityWeek, May 09, 2019

[10] Customers of 3 MSPs Hit in Ransomware Attacks, DarkReading, 6/20/2109

[11] On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective, Aug 2018, Table I.

These are just the payments made to the attackers. It's even more expensive to recover lost computer systems, and to try and maintain services and product deliveries to your customers while those systems are being recovered. In fact it was discovered that some ransomware recovery services secretly pay the ransomware to get their customers' systems back up and running.[12]

These numbers show that unless ransomware attacks become more difficult and expensive to implement, they will continue and likely grow over the coming years. See more on this topic under "**How to stop ransomware**" below.

How ransomware breaches occur

In order to effectively stop ransomware breaches we need to know how they occur. We will focus on the initial attack vectors, because today that is the only proven way to stop these breaches. Ransomware breaches have used the following attack vectors:

- **Remote Desktop Protocol** (RDP) and Remote Desktop Services (RDS) is used to infect un-patched servers and workstations. Un-patched Internet facing servers and desktops are particularly vulnerable to this attack because no user interaction is required to infect the computer. This attack vector was used in the 2017 WannaCry attacks. Recently Microsoft released security updates to prevent a similar vulnerability from being used in new attacks.[13]

- **Email attachments** are used to install ransomware on the recipient's machine or more likely to use the infected machine to gain access to the network and servers by escalating user privileges and dropping ransomware on servers with critical data. These attachments can contain malware that targets un-patched applications or operating systems. The attachments can also target Microsoft Macros.[14]

- **Drive-by websites** contain exploit kits[15] with multiple malware options that can infect a visitor's web browser or plug-ins without any action by

[12] Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers, ProPublica, May 15, 2019

[13] Prevent a worm by updating Remote Desktop Services (CVE-2019-0708), Microsoft, May 14, 2019

[14] Macro malware, Microsoft 5/31/2019

[15] Exploits and exploit kits, Microsoft, 5/31/2019

the visitor. The website can be legitimate without the owners knowing that it has been compromised or one specifically crafted by the attackers to impersonate a legitimate website. The malware exploits target un-patched software such as Web browsers, and plug-ins such as Adobe Flash Player, Oracle Java, etc.

Malvertising, is a modification on drive-by attacks. This is where malware is delivered by online ads, via advertising networks, on legitimate websites and infects visitors with vulnerable Web browsers or other vulnerable Web software. Typically no user interaction is required to infect their computer. [16]

How to stop ransomware

Based on the ransomware attack vectors described above, the following controls should be used to stop these attacks from becoming successful breaches:

- Keep operating systems and applications, including Web browsers and plug-ins, up to date with the latest security updates. There is no indication that any ransomware attack has used a so-called zero day vulnerability, so patching for known vulnerabilities is sufficient.[17]
- Remove all end of life (EOL) software and replace with supported versions.
- Limit the use of administrative privileges.
- Use secure configurations such as those offered by the Center for Internet Security (CIS)[18] or software vendors such as Microsoft[19] and Red Hat[20].

[16] Malvertising, Center for Internet Security.

[17] A zero day vulnerability is one with no security update or other mitigation to stop an attack using this vulnerability. This is not to be confused with a virus for which anti-virus software does not yet have a signature. The latter case is almost always based on a known vulnerability. Zero day vulnerabilities are very rare and almost always created and used by government entities.

[18] Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers, Center for Internet Security (CIS)

The CIS Controls

At Belarc we try to keep things simple, so here's our recommendation on how best to implement cyber security: Establish a process to implement and regularly monitor the Center for Internet Security (CIS) Basic Controls. We like the CIS controls because they are based on lessons learned from actual attacks and breaches and are created by people from multiple industries and government, including the NSA and DHS, who have deep knowledge of all aspects of cyber security.

This is from the CIS:

"The CIS Critical Security Controls (CIS Controls) are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks. The CIS Controls are developed, refined, and validated by a community of leading experts from around the world. Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around 85 percent. Implementing all 20 CIS Controls increases the risk reduction to around 94 percent."

In total there are only twenty controls and the first five are what the CIS calls Basic Controls. Here is a summary listing. Please download the CIS Controls document for a full description of the controls.

- CSC 1: Inventory and Control of Hardware Assets.
- CSC 2: Inventory and Control of Software Assets.
- CSC 3: Continuous Vulnerability Management.
- CSC 4: Controlled Use of Administrative Privileges.
- CSC 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

The CIS Controls document also lists a mapping to the NIST Framework for Improving Critical Infrastructure Cybersecurity and a section on creating Security Governance Controls targeted to senior management and the organization's board of directors.

[19] Windows security baselines, Microsoft

[20] SECURITY HARDENING, Red Hat Enterprise Linux 8.

How Belarc can help

Belarc’s system automatically creates an up to date central repository with detailed hardware, software and security configuration data. Rather than use multiple tools and systems to gather this controls data, often requiring manual efforts, Belarc allows organizations to do this automatically, enterprise wide, on a near continuous basis. See architecture discussion in the following section.

Maps to the CIS Top 5 controls

Belarc’s capabilities map very closely to the CIS Top 5 controls, as follows:

- Complete listing of all hardware including desktops, laptops, servers, virtual machines, tablets and phones. Configuration details include make, model, serial number, BIOS or UEFI, operating system, group policies applied, USB storage device usage, encryption status, and more. CSC 1.

- Complete listing of all installed software including versions and last time used. Ability to automatically compare installed software with standard images or approved software. Flags unused software as candidates to be removed. CSC 2.

- Automatic vulnerability assessment, including end of life (EOL) status, based on published vulnerability data from Microsoft, Adobe, Oracle Java and Apple. CSC 3.

- Detailed information on both local and domain user logins by host and privileges, and the ability to automatically track user account changes such as elevated privileges and new account creation. CSC 4.

- Comparison of configurations to the US Government Configuration Baselines (USGCB). CSC 5.

Belarc’s Intranet Cloud architecture

Belarc's system was designed to operate over the enterprise's Intranet Cloud, either On-Premises or SaaS. Belarc's Cloud architecture is based on lightweight data gathering agents which use the enterprise's Intranet and requires only one server and a single database (see Figure 1 below). The agents communicate directly with a single Belarc server via https (SSL/TLS) protocols, avoiding the need for a hierarchy of servers or scanners and replicating databases. Users can access the data via secure two factor Web browser authentication, based on a need to know.

Allows for rapid deployment and low maintenance

Belarc's Cloud architecture allows for rapid and easy system roll out and extremely low ongoing maintenance. This is because there is no need to install and maintain local servers, scanners and databases. Belarc's products also use the existing TCP/IP network and standard protocols, so that there is no need to manage special router settings across our customer's network. There are also substantial automation features built into Belarc's products which eliminate the need for the manual efforts required by other systems.

Ideal for tracking mobile devices

Mobile devices are becoming ever more useful and pervasive in today's enterprises. Belarc's Cloud based architecture is ideally suited for mobile devices because these devices natively use the Cloud to communicate with the enterprise's IT resources. For example, when remote laptops or phones connect to the enterprise network, Belarc's client will automatically upload their profiles to the enterprise's Belarc server. No additional infrastructure or setup is required.

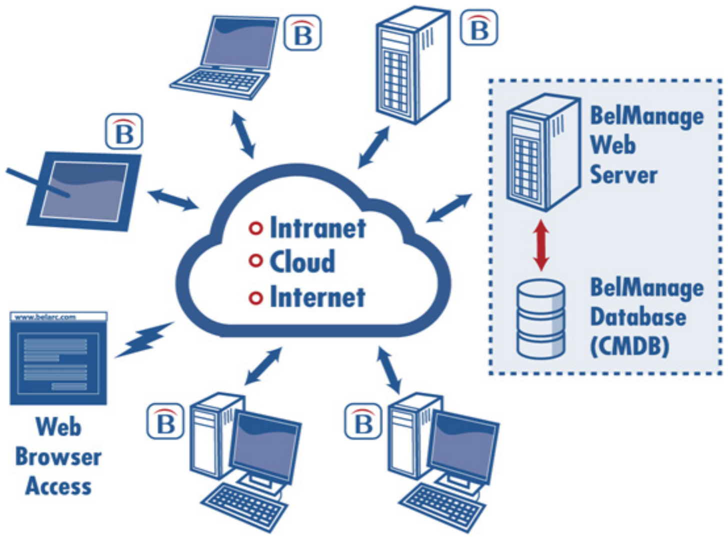


FIGURE 1. Belarc's Cloud architecture

Central repository of configuration data

Another major benefit of Belarc's Cloud architecture is that it automatically creates a central repository, or Configuration Management Database (CMDB) consisting of detailed software, hardware and security configurations. Belarc's CMDB is automatically updated, usually on a daily basis, with accurate and complete information. This obviates the need for gathering data from multiple sources as with a federated CMDB approach.

Proof Positive

Belarc’s products have been successfully used by thousands of both small and large enterprise customers for over eighteen years. Brief descriptions of how some of our customers are using Belarc’s products are described below.

Oakland County Michigan

Oakland County is among the ten highest income counties in the United States with populations over one million people. Oakland County uses BelManage and Data Analytics on nearly 5,000 computers. Belarc’s software was originally purchased for software asset management but was rapidly also used for cyber security monitoring. Oakland County personnel have stated that Belarc’s system was instrumental in helping them avoid the ransomware breaches of the past few years.

Oakland County chose Belarc in an RFI process over many others for the following reasons:

- Belarc is cost effective, both on an initial cost basis and for ongoing maintenance costs.
- Belarc is very responsive to it’s customers requests.
- Belarc’s products are quick to deploy and do not require much if any ongoing maintenance.

Covered California

Covered California is the California Health Insurance Exchange where California residents can shop and purchase health insurance online. Because Covered California handles sensitive personal health information it must meet the HIPAA (Health Insurance Portability and Accountability Act) and California’s cyber security control requirements for healthcare providers who handle personal healthcare data.

Covered California uses their BelManage and Data Analytics software on 2,500 computers to accomplish software license management and cyber security monitoring. Belarc’s software is implemented for Covered California as a SaaS offering.

Security Snapshot

Security Snapshot offers cyber security services for independent financial advisors and helps them meet the SEC (US Securities and Exchange Commission) and FINRA (Financial Industry Regulatory Authority) cyber security requirements. The independent financial advisors are often small firms with less then ten employees, but because of the personal financial data that they handle, these firms need to meet stringent and complex cyber security controls.

Security Snapshot uses BelManage to automatically monitor over 6,000 computers used by these independent financial advisors and report to these firms on a regular basis as to their cyber security compliance status.

Railinc

Railinc is a subsidiary of the Association of American Railroads and offers IT and information services to the railroad industry. Railinc runs BelManage and Data Analytics on 1,600 host machines, mostly Linux and Windows servers, for configuration control and cyber security monitoring in addition to software license management.

US Federal Aviation Administration (FAA)

The US FAA deployed Belarc throughout their enterprise on over 57,000 IT assets in under one month. Their initial justification for Belarc was for software license management and the system has already helped the FAA identify over $million in un-used Microsoft desktop software. Belarc's data also allowed the FAA to effectively negotiate a $tens of millions overage request from IBM. Belarc's system is also being used in their Microsoft EA true up, including desktop and server software, Oracle database software, IBM, Adobe, ESRI (ArcGIS), and other high value software agreements. As a by-product of the data Belarc's system collects, it is also being used to track many of the NIST 800-53 security controls, and the Major Applications for the Portfolio Management process.

USAF 844th CG

The USAF 844th CG, covering over 25,000 IT assets at the Pentagon JCS and Joint Bases Bolling and Andrews, has been using Belarc's system since 2007 for managing their enterprise software license agreements and to monitor their security controls. BelManage was initially used to offer authoritative data for their Microsoft EA license true-up, resulting in a $2.7 million annual savings on this ELA alone. It was submitted as for a Best Practices Nomination. In addition Belarc is used to help monitor the USAF's vulnerability status and other security controls.

Joint Special Operations Command (JSOC)

JSOC is a sub command of the US Special Operations Command and is charged to study Special Operations requirements and techniques, ensure interoperability and equipment standardization, plan and conduct Special

Operations exercises and training, and develop joint Special Operations tactics. JSOC also oversees the Special Mission Units such as the Army Delta Force, Rangers, Navy Seals and others.

A JSOC contractor originally brought in BelManage and installed it on approximately 19,000 host machines to help with their cloud migration program by identifying all software applications installed and whether they have been used or are EOL. Belarc is also being used for cyber security monitoring of the DISA IAVAs (Information Assurance Vulnerability Alerts).

Catholic Relief Services (CRS)

CRS is located in 101 countries on five continents, offering humanitarian services. Their BelManage system runs on 5,000 clients often located in very remote areas and updates are sent to their BelManage server when connections are possible. Their BelManage system is used for ITAM, SLM, configuration control and IT security.

Pontificia Universidad Católica del Perú (PUC)

PUC is a private university located in Lima, Peru with over 27,000 students and is ranked as the top academic university in Peru. PUC uses BelManage on over 7,300 of their IT assets, including desktops, laptops and servers. PUC uses their Belarc system for software license management, cyber security audits, software configuration control and service desk support.

Summary

Ransomware has had a dramatic impact on U.S. state and local government organizations, healthcare providers, and large international enterprises. Ransomware attacks will likely continue or even increase because the attackers make a lot of money and it’s relatively easy to accomplish. This state of affairs will continue unless both public and private organizations make these breaches more difficult to accomplish. When we analyze the actual security breaches it is clear that to achieve real security, organizations need to follow good cyber security hygiene practices. This can best be accomplished by implementing and continuously monitoring proven security controls from organizations such as the Center for Internet Security (CIS). Belarc’s system is ideally suited to accomplish this in an automated and low cost fashion.

Contact Us:

For additional information please contact us:

Belarc, Inc.
Two Mill & Main, Suite 520
Maynard, MA 01754 USA
Tel: (+1) 978-461-1100
Email: info@belarc.com
Web: https://www.belarc.com