Blueliv.

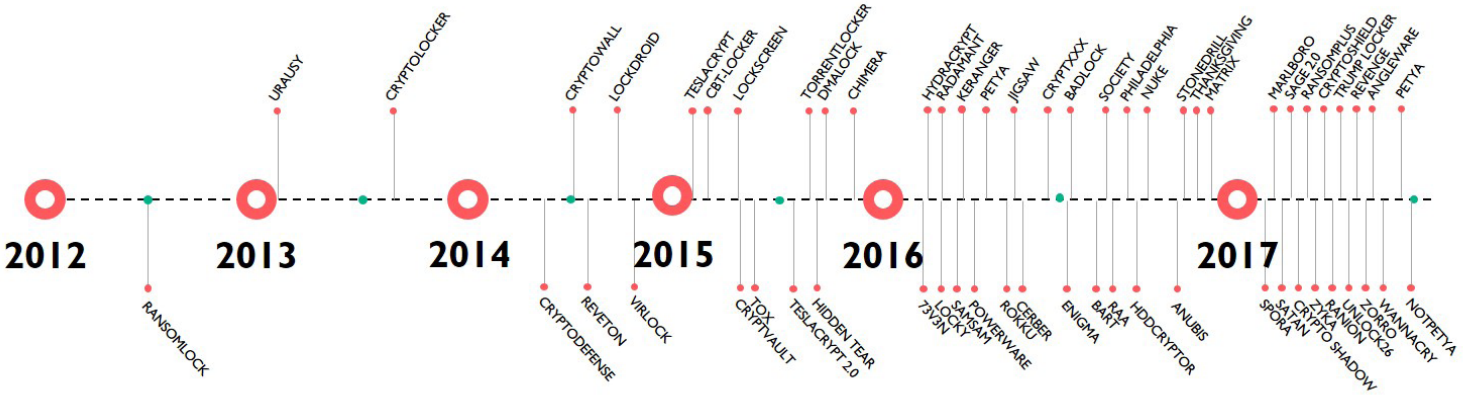
PREVENT AND MITIGATE RANSOMWARE WITH BLUELIV

Ransomware is on the rise and can potentially impact any company or individual. In 2016, it became a $1 billion crime industry, attracting an increasing number of cyber criminals.

Different types of ransomware affect different types of devices, but they operate the same way. Ransomware is a piece of malicious software that encrypts files or blocks computers, and afterward demands a ransom payment to recover the data and unlock the device.

In some cases, ransomware encrypts your data and then proceeds to send the key to a dead crime server. If this server never receives the key (no connectivity, dead server...), you will not be able to recover your files even if you pay, simply because even the author doesn't have the key for decryption.

So, the best approach to fight against Ransomware is to concentrate on avoiding it altogether, or trying to mitigate its impact.



HOW TO PREVENT RANSOMWARE

Blueliv can provide some generic tips to face these types of threats:

- Be aware of what you receive as an email attachment and verify files before clicking them
- Verify the source of the email and think about whether you were waiting to receive such an e-mail
- In the same sense, beware of files downloaded from public sites, even if you think that they are innocuous documents
- Installing and keeping an AV system updated (this probably won't be enough to block new ransomware versions because viruses are constantly morphing to evade signatures)
- Patch, patch and patch your applications, so no "entry doors" are left open!

HOW BLUELIV CAN HELP YOU TO PREVENT RANSOMWARE

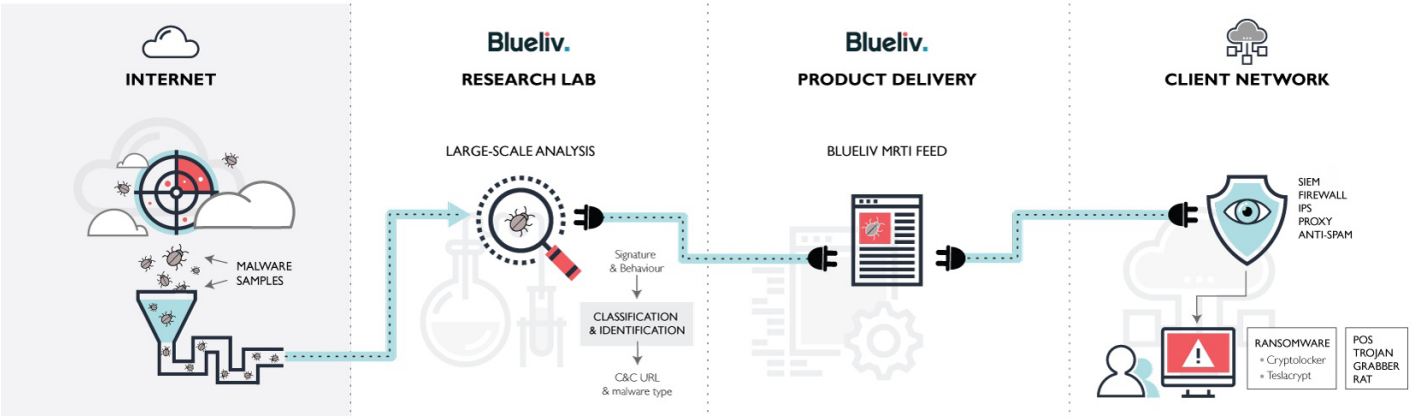
Blueliv scours the web and the dark web to detect emerging threats outside your network.

One outcome of this process is Blueliv's Machine Readable Threat Intelligence, a feed based on a large-scale malware analysis engine that constantly analyzes malware samples, performs classification & identification of malicious content, extracts crime server URLs, all of which are compiled into one single feed that provides you information about crime servers, Exploit Kits, Malware Hashes and Bad Reputation IPs.

This information enables you to block threats before they affect your users and assets

BENEFITS

- High quality information originated from a myriad of sources and millions of malware samples (highly contextualized information validated by Blueliv's processes)
- Intelligence delivered in real-time (continuous updates available)
- Easy integration into your existing security solution (API in different formats, including STIX/TAXII)



- Free **Blueliv Malware Analysis Sandbox:** If you suspect one of your files is infected, get it analyzed for free with the Blueliv sandbox. Join Blueliv Threat Exchange Network, upload and analyze the sample to find out if it is infected by a known malware. Benefit from a report that includes the connections that the sample made during runtime analysis.

WHAT TO DO TO MITIGATE RANSOMWARE ATTACKS

- Perform App whitelisting to allow or block program execution
- Improve and boost your Backup and Restoring system

HOW BLUELIV CAN HELP YOU TO MITIGATE RANSOMWARE ATTACKS?

The Blueliv Team has successfully helped some customers to decrypt files that have been encrypted. Feel free to contact us and ask for help! Keep in mind that paying the ransom is not always the only option, and that there might still be hope for your files.

Ransomware has been around for a decade, but has evolved in recent years to become an increasingly potent threat capable of extracting ever larger ransoms.

You can protect your organization before they become ransomware targets.
If you want to know more about our solutions we'd love to talk about it with you.

Get in touch with us at sales@blueliv.com

twitter.com/blueliv

es.linkedin.com/company/blueliv

www.blueliv.com

ABOUT BLUELIV

Blueliv scours the web, the deep web and the dark internet to deliver fresh, automated and actionable threat intelligence to organizations across multiple industries to protect their networks from the outside in.