Prevent ransomware attacks from taking down your business and defend your data

Trusted partner for your **Digital Journey**

Atos

ATOS at a glance

Introduction

The exponential advancement of technology and digitalization are creating new possibilities for organizations to take advantage of alternative business models. Moreover, organizations are operating amidst widespread disruption, which stems from changes in society and regulations, coupled with the increased threats in information security.

Drastic emergency situations provide a conducive environment for criminals to perform cyberattacks. For example, with COVID-19 there has been a massive surge in cybercriminal activities. Attacks have been targeted not only against those fighting in the frontline (hospitals) but also those who are innocent and vulnerable. Ransomware is probably the most publicized and discussed IT outage cause for the past years. Ransomware attacks today are clearly on the rise and the risk of organizations' sensitive data being stolen is even higher. Hackers perform these attacks to demand a ransom in exchange of undoing their attacks. However, paying the ransom does not always ensure that hackers will uphold their word.

According to Interpol, the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure. "Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19", said Jürgen Stock, INTERPOL Secretry General.

Europol, the European Union's law enforcement agency says that COVID-19 pandemic has made organizations like hospitals, governments and universities, more conscious about losing access to their systems and more motivated to pay the ransom.

Criminals take advantage of this situation by:
- running faster and more ransomware attacks;
- recruiting collaborators to help them maximize their impact;
- offering ransomware-as-a-service on the dark web.

60%

Increase in targeted ransomware attacks in 2019

Source: Broadcom Symantec Enterprise

120$

Monthly subscription is the price for Ransomware-as-a-service package Ranion on the darknet marketplace

Source: https://www.bankinfosecurity.com/

20$

Was the price for a Remote Desktop Protocol (RDP) server credential located in Europe and in the U.S on the darknet marketplace

Source: https://www.bankinfosecurity.com/

Ransomware: What is it and who are the most recent victims?

Ransomware is a malicious software that encrypts infected system and restricts access to a computer and/or files on a computer until a ransom is paid. It can be downloaded or accessed in more and more creative ways and then passed between users and computers much like a traditional virus but much more evolved.

These attacks exploit security vulnerabilities like weak Remote Desktop Protocol (RDP) credentials or use phishing emails to infect computers. When a computer is infected it enforces restrictions through encryption and prohibits access to certain areas of a computer or environment. Cybercriminals are very creative, with Ransomware-as-a-Service (RaaS) cybercriminals use the Software-as-a-Service model to deliver attacks on demand, in an easy way, by almost anyone that wants to act maliciously. RaaS works similarly to SaaS when it comes to availability, subscription and promotion, but on the dark net. There are many variants of the Ransomware which belong to two main categories, the ones which lock access to a computer preventing the victim to use it "Locker-Ransomware" and the most common ones which encrypt sensitive data preventing access to files or data "Crypto-Ransomware".

Some of the most popular "Crypto-Ransomware" attacks include:

Wanna Cry

WannaCry was a high-profile attack that exploited vulnerabilities in software. Normally, when vulnerabilities come to light, software vendors write additional code called 'patches' to cover up the security 'holes'. WannaCry was a self-replicating ransomware attack that started in May 2017 and targeted unpatched Microsoft Windows environments. It affected over 200,000 machines in 150 countries, with collateral damage to public and private sector organizations and potentially hundreds of millions of pounds in operational losses.

WannaCry targeted Microsoft Windows computers and exploited vulnerabilities in the Microsoft implementation of Server Message Block (SMB) protocol and encrypts data.

NotPetya

NotPetya started in June 2017 and targeted machines initially through updates to popular financial software after its source code was compromised. It affected companies in Ukraine and global companies with subsidiaries there, with costs totaling hundred of millions of euros.

NotPetya targets Microsoft Windows computers and encrypts data, it exploits a Microsoft vulnerability and affects organizations that have not applied security patches available from Microsoft. It's delivered by email phishing campaigns.

Maze

Encrypts files, modifies file extensions with random data or some identification of the victim and leaves a ransom note threatening the victim to publish information on the internet.

The ransomware uses RSA-2048 and ChaCha20 encryption and requires the victim to contact the threat actor by email for the decryption key. The threat actors behind the malware are known to have attacked multiple sectors including government and manufacturing and threaten to release the company's data if the ransom is not paid.

Wasted Locker

It's attributed to the "Evil Corp" cyber crime group. It interacts with Windows APIs to avoid being detected by security software such as anti-ransomware. It's reportedly using Windows cache to encrypt documents in memory and foul detection.

Net walker

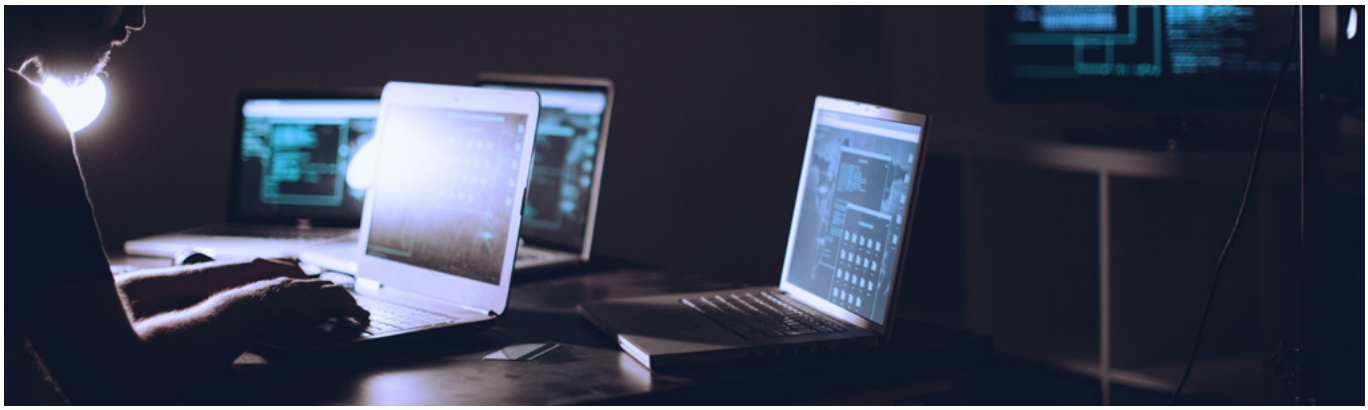
Also known as "Mailto", it targets networks and encrypts Windows devices and data; it deploys an embedded configuration that includes a ransom note, the ransomware has been active since September 2019. Netwalker was transitioned to RaaS delivery model recently.

Exorcist

Encrypts files, modifies file extensions with random data, changes wallpapers and leaves a ransom note. A deadline is given to the victim to pay the ransom.

https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware.html

Ransomware attacks have been a lucrative practice for many hackers with unfortunate companies being forced to pay up for the safe return of their IT infrastructure. And with so many organizations failing to back-up properly, or often paying up out of embarrassment it will continue to be a potential goldmine for cybercriminals.



Ransomware creates significant disruptions for organizations causing loss of income associated with business downtime and recovery. In addition to which, the victim also bares the payment of ransom and reputational damage.

Top 3 Recent Ransomware Attacks

In July 2020, Garmin was infected with a relative new ransomware, the WastedLocker, taking down several services apps, website and call centers. Garmin reportedly paid millions of dollars to the attackers[4].

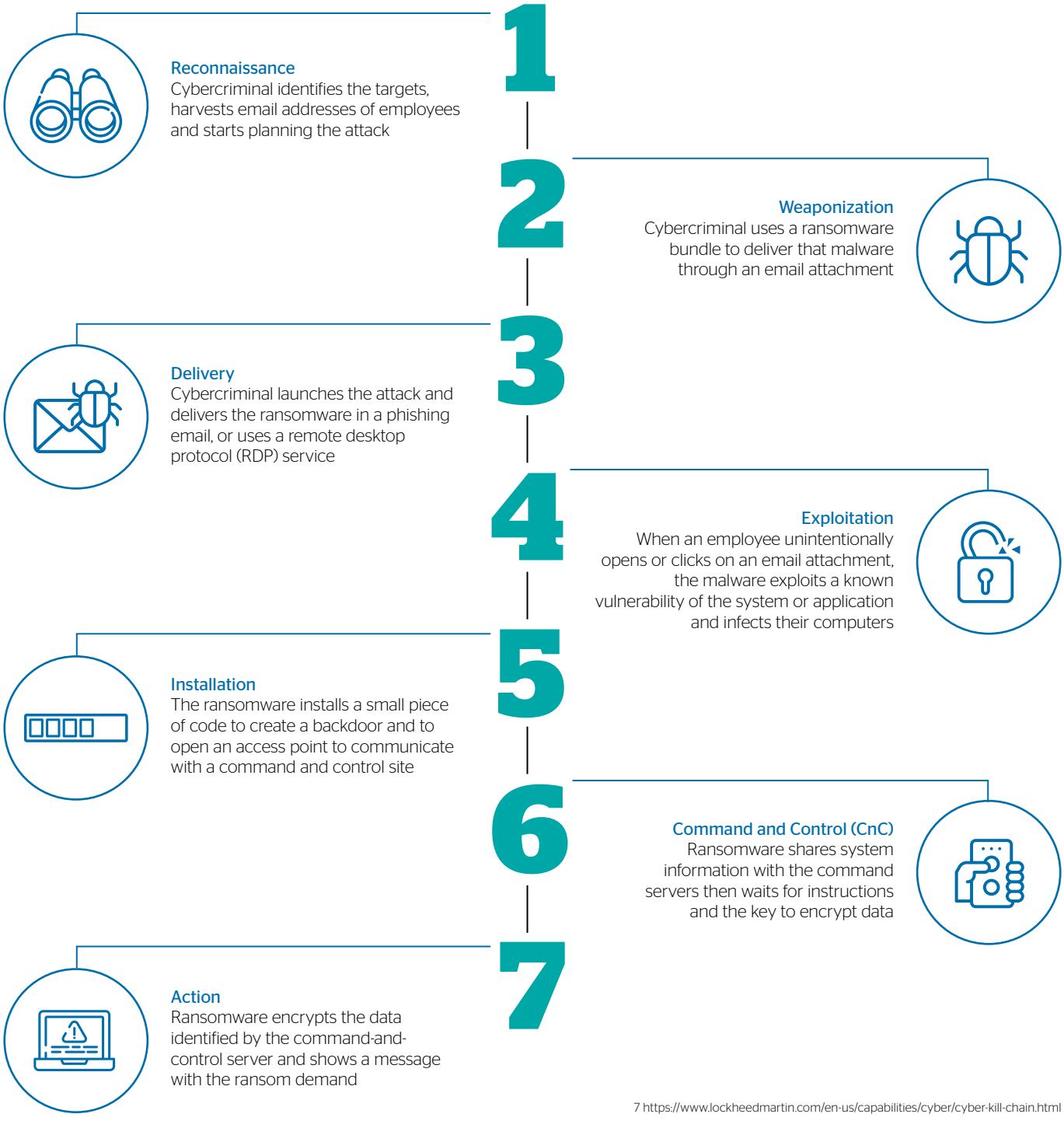
In July 2020, Telecom Argentina suffered from a ransomware attack. It's reported that hackers demanded $75 million paid in Monero privacy coin. Hackers caused extensive damage to the company's network after they managed to gain control over an internal domain admin. Thus, they could spread and install their ransomware payload to more than 18,000 workstations[5].

In August 2020, Canon suffered a Maze Ransomware attack involving the theft of 10TB and impacting numerous services such as Canon's email, Microsoft Teams, USA website, and other internal applications[6].

4 https://www.somagnews.com/garmin-may-have-paid-ransom-after-cyber-attack/
5 https://www.cpomagazine.com/cyber-security/hackers-demand-hefty-ransom-after-successful-ransomware-attack-on-telecom-giant/
6 https://www.forbes.com/sites/daveywinder/2020/08/05/has-canon-suffered-a-ransomware-attack-10tb-of-data-alleged-stolen-report/#987af1c499ec

Sequence of events involving a ransomware attack

The Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity[7]. The Seven Stages of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures. This chain helps to understand and respond to a ransomware attack.



7 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

How to stay safe from ransomware

Ransomware attacks can come from anywhere and anytime. Given the increasing number of such attacks, organizations must realize that being proactive rather than reactive is the best solution. Most organizations follow the best practices listed below; however, they are not enough in majority of the cases.

Education - Don't click these links!

Ransomware needs some way of accessing your network, this is mostly going to be through your endpoints, your non-IT employees. You must educate the workforce; this is not just an IT department issue, it's vital that you train your employees to recognize suspicious phishing emails through simulation exercises to defend against attack delivery.

The risk:
It only takes one employee to make the mistake of opening a phishing email and infecting the company's network.

Deployment of secure email/web gateways

You can use this technique to defend against ransomware attacks delivered through email.

The risk:
Security web/email gateways are unable to detect a new strain of malware, because it does not have the signature.

Updating everything

Regular scanning of your systems and patching high priority vulnerabilities, helps defend against holes exploited by a ransomware. There are releases all the time around preventive patches. These releases will keep vulnerabilities at bay just by adhering to an update schedule. Antivirus, Firmware, Applications and Operating Systems all play a huge part in the prevention of malicious threats.

The risk:
Ransomware can be delivered with day 0 methods, and it is difficult to guarantee 100% patched systems in our complex environments.

Monitor DNS Queries

After a ransomware infects a server/endpoint, it typically calls home to a command and control (CnC) sever to exchange encryption keys. Monitoring DNS queries to known ransomware domains (e.g. "killswitch") and resolving them to internal sinkholes can prevent ransomware from encrypting files.

The risk:
DNS servers are unable to block any unknown CnC domains used by new ransomware attacks. In addition, modern ransomware attacks account for DNS monitoring and take evasive actions.

Back-up, back-up, back-up

Back-up and recovery are the 101 of cybersecurity. Unfortunately, some organizations do not have the resources to update or integrate their new IT environments into existing security policies or into their back-up plans. That makes them very vulnerable to ransomware attacks.

And still, there may be times when all your security defenses fall short, and the ransomware attack succeeds in encrypting all your business-critical data. The best way to recover from a ransomware attack is to maintain a secure backup and also have a clear recovery plan that enables you to restore your business-critical data.

The hurdle:
Restoration is expensive and time consuming. In addition, you still need to determine if the malware is still in your system, and you need to identify and close the entry point, or restoration will only be a temporary fix.

How to stay safe from ransomware

There is no single solution for making sure that an organization is safe from attacks. In addition to the preceding list, at Atos, we believe in an approach that incorporates all the following controls to effectively block any unknown malware (ransomware binaries) from taking your data hostage.

Implementing a risk assessment

Understanding the value, location and security of your infrastructure and data can help you see where gaps in security or back-up processes might be lurking.

Understanding the changes & associated threats that your digital transformation is introducing, is also a must.

Adopting security policies around identity-based security

Controlled identity and access management does reduce exposure to ransomware attacks. It's necessary to configure your user accounts in a far more stringent way where most restrictive set of privileges possible are granted to perform a task required for their job roles, according to the "need to know" principle, not further.

Compromised credentials make life easier for cybercriminals and expose organizations to multiple risks. It has been reported that new version of FTCODE ransomware includes a new functionality to steal credentials from browsers and email.

Implementing application whitelisting

Identifying trusted applications is very important to prevent unauthorized applications from being installed. Enforcing "applications whitelisting" is a must for Cloud Native Applications deployed through Infrastructure as a Code (IaaC) architectural principles, giving organisations the confidence that components of the infrastructure never deviate from the intended configuration.

Enforcing fine-grained access to folders and files

Fine-grained control access to your business-critical data defines who (user/group) has access to specific protected files/ folders and what operations (encrypt/decrypt/read/write/directory list/execute) they can perform.

Some malwares depend on escalating privileges to gain great system access. Appropriate access control solutions can bar privileged users from examining and even accessing resources.

Encrypt Data-at-rest

Encrypting sensitive data is a must. Even if the data falls in wrong hands, encryption ensures data privacy and confidentiality.

Encryption protects data at rest irrespective of where it resides (On premise data centers or in public/private clouds). This makes the data worthless to intruders when they steal business critical or sensitive data and threaten to publish it for ransom. In addition, some ransomware selectively encrypts files so that it doesn't take systems entirely offline. Others look for sensitive data and only encrypts those files. In such cases, encrypted files aren't possible to scan by the malware and are not attacked.

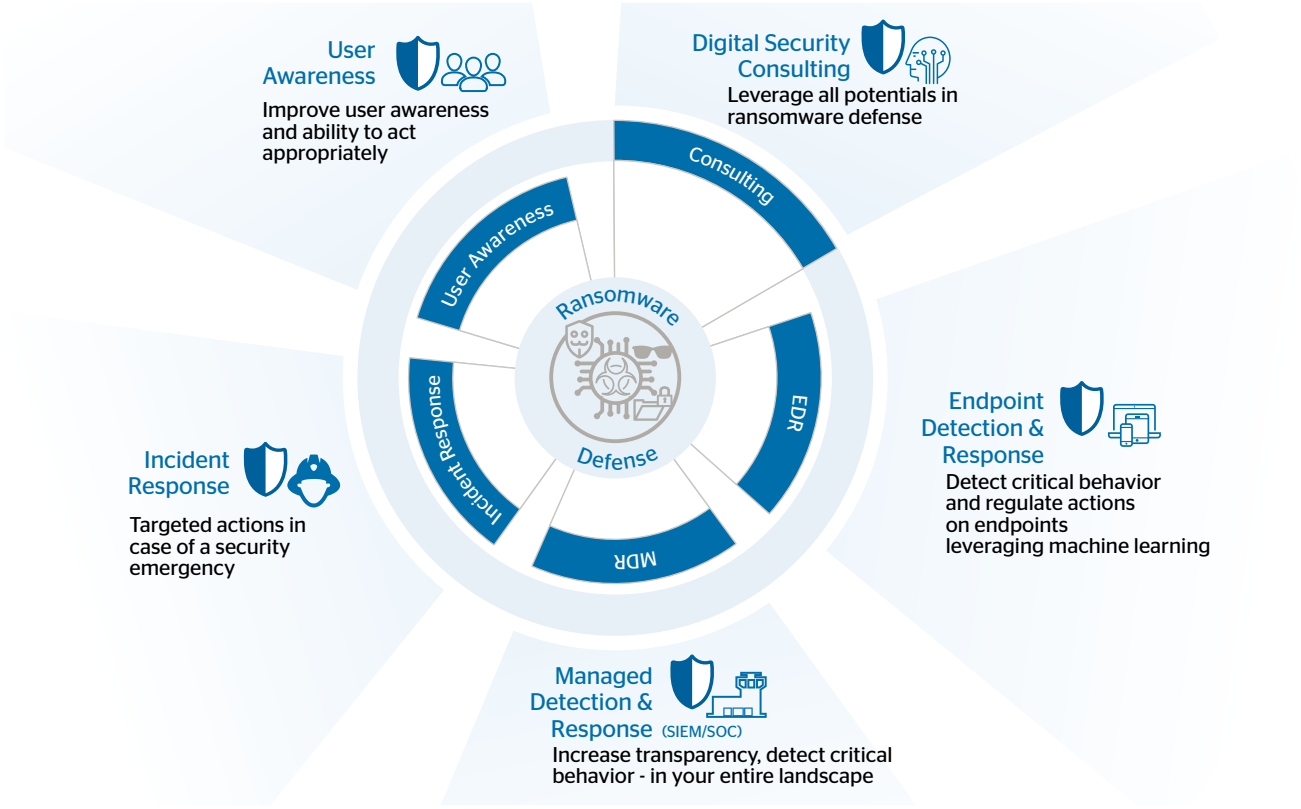
Leverage big data and supercomputing capabilities

Prevent breaches from happening by detecting and orchestrating automated security actions to neutralize cyber threats before they strike is key. With the new technologies it's possible to shift from a reactive and proactive model to a prescriptive model, focused on analytics patterns in order to identify emerging threats and automate the security control responses.

How does Atos solutions help you protect and defend against ransomware

Atos offers a comprehensive set of end-to-end services that enable organizations to leverage the potentials of Digital Security.

Reducing the attack surface by strengthening the important "human security component" in the first line of defense is the starting point. Transparency, significant insights, detection of critical behavior leveraging machine learning and regulating actions are the heartland of ransomware defense on your endpoints and in your entire landscape.



Ransomware attacks rely on being able to spread and infect all-over a landscape. Having the Zero Trust conception as overall objective, Atos Digital Security Consulting focusses on robust and secure topology, adequate identity and authentication regime as well as suitable application of best practices. Appropriate governance and strategy for an emergency complement your framework.

Where are you on your journey to Zero Trust?
Penetration Testing reveals your most urgent fields of activity!

Ultimately, effective ransomware defense is always built on the convergence of a plurality of security disciplines.

RANSOMWARE DEFENSE

Atos concerted DIGITAL SECURITY

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of over € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos operates under the brands Atos and Atos|Syntel. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
https://atos.net/en/solutions/cyber-security

Let's start a discussion together

For more information: https://atos.net/en/solutions/cyber-security

CT-210330-JR-WP-RANSOMWARE DEFENSE GER