
allot
See. Control. Secure.
Threat Bulletin
Atrimunte
December 2020

Introduction

Atrimunte is neither a computer virus nor malware, but a malicious webpage hosted at www.atrimunte.com (now no longer active). This webpage serves the simple purpose of redirecting visitors to other malicious websites. It is essentially a dynamic waystation that launches unsuspecting users into other harmful domains.

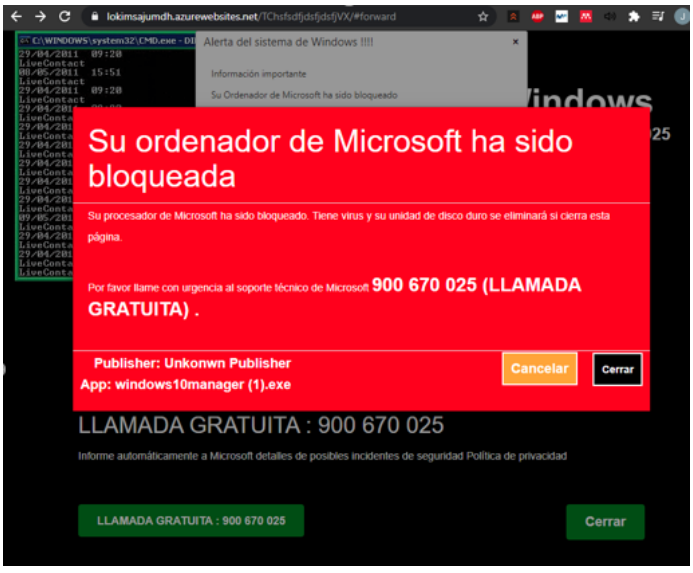
URL redirection is a common technique in the online sphere. It is used legitimately to redirect visitors to specific subpages based on geolocation or other user characteristics. Cybercriminals use redirects to trick users and skip them through a series of domains before arriving at the malicious destination. This helps them cover their tracks and quickly make changes to any part of the chain to stay ahead of security measures. As soon as one malicious domain is identified and blocked, they easily swap that chain in the link.

How are Users Infected?

In the case of Artimunte.com, users were directed there as a result of a prior infection on their device or via pop-up ads from a previous adware infection. Pop-up ads are usually considered a mere nuisance, but little more. Atrimunte is a perfect example of just how much damage they can cause. Previous adware infection was likely the source of much of the traffic sent to Atrimunte during the July 2020 attack.

Malicious Activity

During the active attack campaign in Q3 2020, Atrimunte likely redirected to multiple malicious pages.



One redirect was to a website designed to look like a perfect replica of Amazon.es, the official Amazon site for Spain, and tricked users into submitting their payment details.

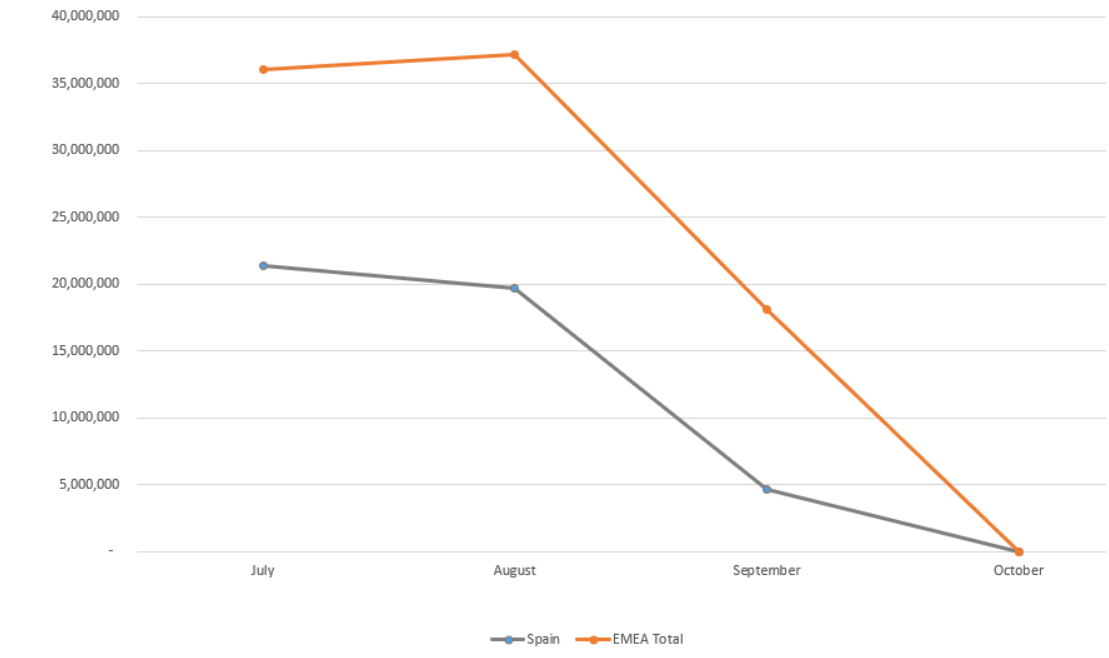
Another redirect was to a very sophisticated Vishing attack. Vishing is a term for a type of phishing attack that uses VoIP technology to create fraudulent phone numbers. In this attack, Atrimunte launched an alarming pop-up message that appeared to be from Microsoft, claiming a virus has been detected on the user's computer, their browser has been blocked in order to contain the spread of the virus, and that they should call the number which appeared in the message if they wish to rectify the situation. Users who called these numbers and provided their bank or credit card details in order to "renew the account" or "remove the virus" did not know that they fell victims to a "Vishing" (Voice Phishing) attack by cyber criminals. Sometimes the phone numbers themselves were premium numbers and the callers would unknowingly be charged a high fee for every second they were on the call (premium toll numbers). This Vishing attack shows how cybercriminals invest in building sophisticated, multi-step scams that easily fool even the most vigilant user.

Allot Secure Atrimunte Blocks

During Q3 2020 Allot Secure protected users in Europe from accessing the malicious Atrimunte domain 91,420,432 times

Atrimunte first bleeped on the Allot Secure radar in July 2020, across Europe, primarily in Spain. The first attack appears to have lasted about one month and the website is offline as of publication. Allot Secure has detected and pre-blocked 91,420,432 cyberthreat events which involved the Atrimunte URL.

Allot Secure Atrimunte Blocks: July-October 2020



Conclusion

Protect Subscribers with Allot Secure

Allot Secure allows CSPs to protect their subscribers from all types of cyberthreats by offering security as a service (SECaaS) from the network. Up-to-date threat intelligence and in-line anti-virus scanning protects users from banking trojans like Ginp, and all types of malware, crypto jacking, ransomware, and IoT specific attacks such as Mirai and its variants.

Allot Secure unifies network-based security, home and business gateway security and security clients into the CSP's own branded security service. It delivers a seamless customer experience through a single interface for policy setting, reporting, and event handling.

To learn more about how service providers can increase customer satisfaction, NPS and ARPU by offering Allot Network Security Solutions, download the Telco Security Trends Report:

How Effective are CSP Security Services for the Mass Market?
or watch this video: **How Allot NetworkSecure Works**.