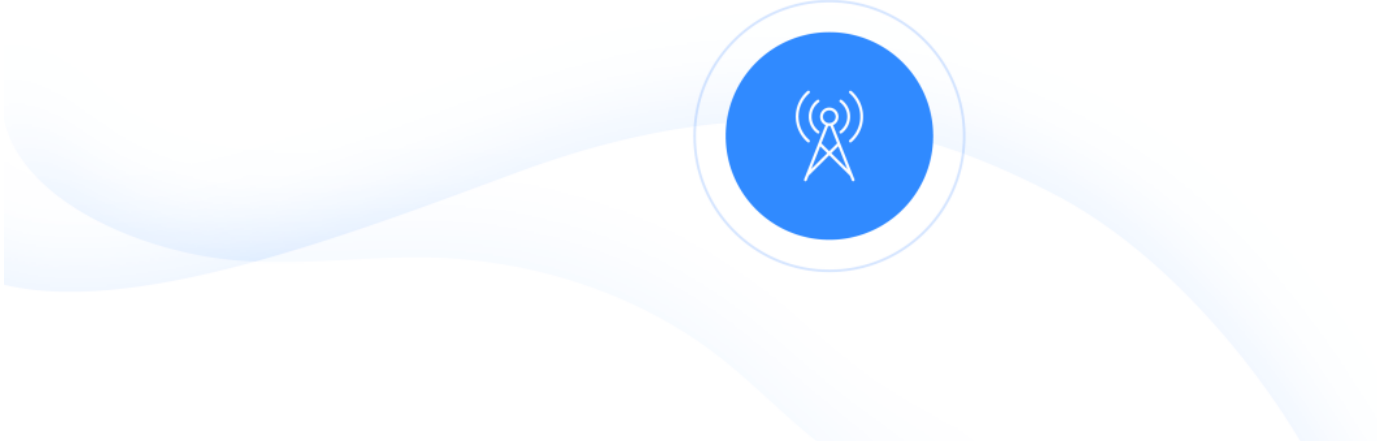
Top Cyber Threats to the Telecom Industry

Written by Intezer - 5 May 2022



In our interconnected society, the telecom industry is responsible for keeping the world connected 24/7. The telecommunication infrastructure uses satellites, internet providers, mobile phones, cloud, and IoT devices to achieve this goal. This widespread adoption makes this sector very attractive to cybercriminals.

Cyberattacks against telecom companies have risen because one successful attack gives attackers access to sensitive information on millions of customers. This valuable information can be sold on the dark web or used by nation-sponsored groups for collecting intelligence on other countries. This article will overview some of the most pressing threats for telecom companies and what you can do to prevent them.

The Telecom Cybersecurity Threat Landscape

The diversity of the services offered by telecom industries comes with increasing cyber risks. The major attack vectors threatening telecom companies are Denial of Service, malware, and ransomware. Attackers take advantage of the single entry point and maximum effect to carry out successful attacks. Here are recent significant threats:

1. ShellClient RAT

In July 2021, researchers discovered advanced malware targeting global aerospace and telecommunications companies. Called ShellClient, the malware is a never-seen-before RAT(Remote Access Trojan) that is highly evasive and designed to steal sensitive information from compromised computers.

The Iranian group MalKamak was identified as the authors and operators of this threat. Based on the research evidence, this malware has been active since 2018.

1. LightBasin (aka UNC1945).

This Iranian hacking group infiltrated 13 telecommunications operators to collect signal intelligence and highly sensitive information such as subscriber information and call metadata. According to researchers, the LightBasin activity cluster started in 2016 and was disclosed in October 2021.

1. LAPSUS$

T-Mobile was breached multiple times by the LAPSUS$ cybercrime group in March 2022, ultimately stealing source code for a range of the telecom company's projects, as first reported by KrebsOnSecurity.

While LAPSUS$ is known for stealing data and holding it for ransom (while threatening to not to publish or sell it), the report indicated the intent in this attack on the telecom provide was to steal and leak T-Mobile's proprietary computer source code.

(T-Mobile was also hit by another threat actor in December 2021, with the the Polish branch of T-Mobile suffering a DDoS attack as attackers attempted to paralyze the network by flooding it with high data traffic volumes.)

1. Macaw ransomware

Sinclair Broadcast Group, which operates 185 local TV stations across the U.S., was hit by ransomware called Macaw in November 2021. The attack was launched by a known Russian group called Evil Corp.

1. VermilionStrike

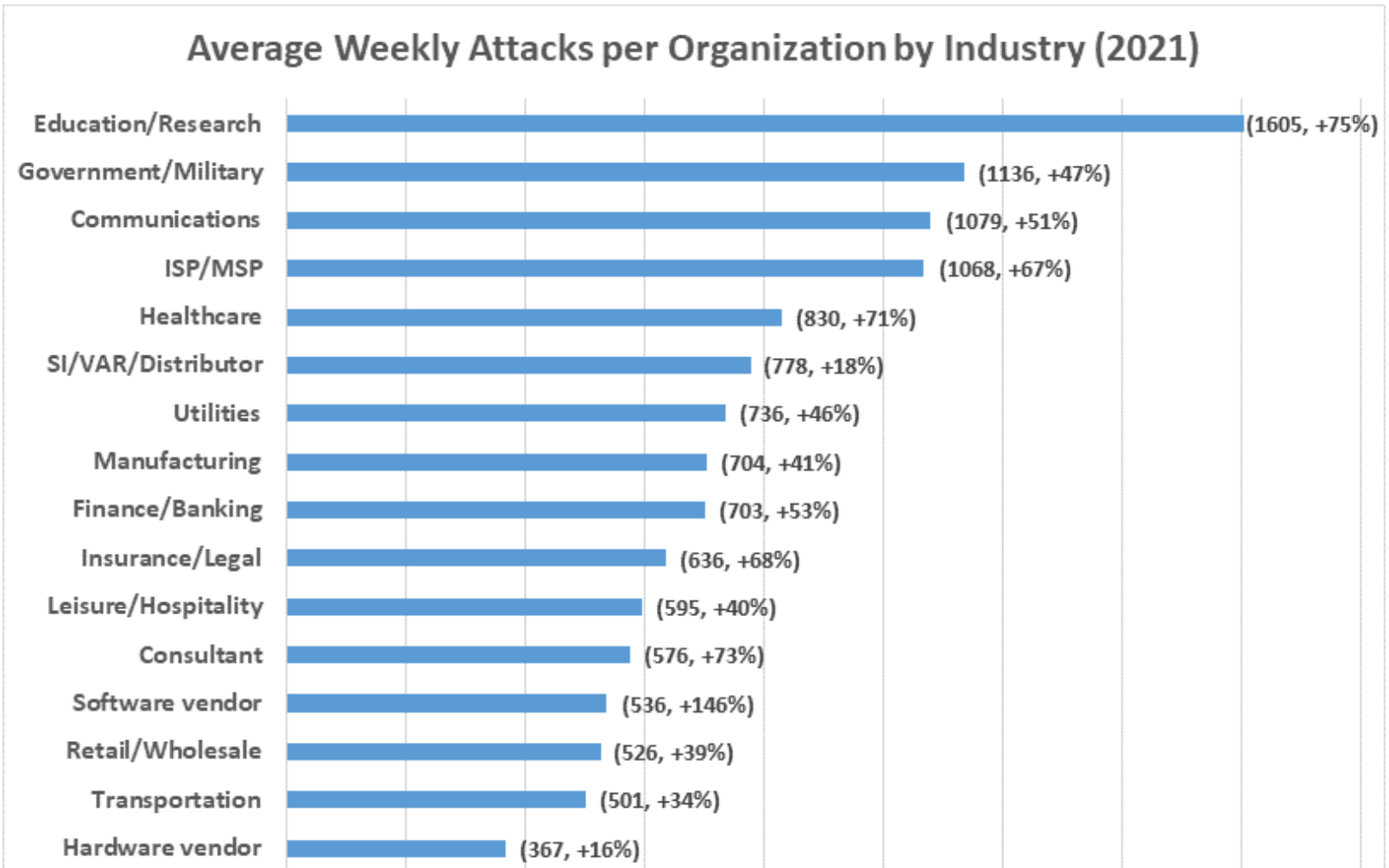
Intezer's research team discovered a sophisticated threat we called VermilionStrike. The Linux version has been active in the wild since August 2021, and it targets specific industries, including telecom companies. The VwermilionStrike threat is the re-implementation of Cobalt Strike Beacon (a popular red team tool for Windows) written from scratch, and it targets both Linux and Windows systems.

The threat escalation is a cause of concern for telecom companies that look for ways to protect themselves from the disastrous consequences of malware ransomware. To understand how to protect your organization, first, we need to analyze the motivations behind the attacks and the most dangerous companies' threats.

Why is the Telecom Industry so Attractive to Attackers?

The interconnectedness of telecom networks makes them an ideal target for attacks that aim to provoke the most damage with the least effort.

Communications are in third place in average weekly attacks per organization.



Source: Check Point

Today's threats against telecommunications are the result of a combination of typical IP-based threats on an industry that still has legacy technology. As 5G technology advances, the threat surface will only expand, giving attackers more opportunities. This leaves cybersecurity teams at telecom companies looking for ways to leverage new technology and automation to streamline workflows so they can stay ahead of attackers in the face of new threats and an increasing amount of alerts to triage.

Top Threats Affecting the Telecom Industry

Telecom companies typically have to triage a high volume of EDR alerts, constantly investigate URLs and attachments from phishing emails, and engage in threat hunting to proactively identify malicious code. Here's a few of the focus areas that telecom companies are boosting their security.

Supply Chain Threats

Telecom and especially mobile operators usually rely on external vendors for infrastructure, products, and services that complement their own. Third-party vendors may pass risks and vulnerabilities to the rest of the supply chain. An attacker needs only to compromise a weak link on the chain to affect the entire supply chain. 2021 was a year with plenty of examples of this type of attack, for instance the high-profile Solar Winds attack.

Here are some tips to protect your software supply chain from attacks:

- Be proactive about your supply chain security and threat hunting.
- Scan your software for any embedded malicious code before you release it, using a tool that's capable of detecting snippets of malicious code within any trusted code that you've privately indexed.

Cloud Threats

Many telecom networks are using cloud computing to support operations. Although it is deemed more secure than on-premises systems, a successful exploit of a server vulnerability can compromise multiple virtual machines. A cloud can be a victim of misconfiguration.

Recommendations:

- Use a runtime cloud workload protection platform to get high-level visibility into the security of your cloud infrastructure, alerting you about any malicious or unauthorized code.
- Enforce security controls over your shared responsibility of cloud services.
- Confirm your cloud providers comply with industry-standard certifications.

IoT Threats

Attackers use the Internet of Things devices as an entry point to networks. They may use the same technique to attack different devices, downloading more malicious code as they expand the attack surface. Some vectors used to compromise IoT devices include weak credentials, vulnerabilities, and exploit kits.

Recommendations:

- Implement IoT device monitoring processes, with processes to automatically triage alerts and extract data (including IoCs and TTPs) from any detected files or URLs.
- Secure internal IoT devices and segment the network.

Phishing Threats

Phishing emails are a top concern for telecom companies, targeting unsuspecting employees who can be lured into clicking a link or opening a malicious attachment.

Telecom cybersecurity teams must build efficient processes to investigate reported and detected phishing emails, which may require scanning and extracting IoCs from a high volume of URLs and suspicious files. To keep up with the number of phishing alerts, many teams are incorporating more automation to remove some of the manual work typically involved in their workflows.

Recommendations:

- Create a phishing investigation pipeline, integrating automation into your abuse inbox or email security system to automatically classify file attachments or URLs and accelerate response in phishing incidents.
- Ensure your security awareness training program covers phishing and how employees should report suspicious emails.

What's Next?

Ultimately, telecom organizations are stepping up their security efforts, incorporating more automation into their workflows to keep up with alert triage, incident response, and threat hunting.

Talk with us about how your security teams can use Intezer to stay ahead of attackers targeting your industry


Intezer

Track the latest malware variants and threat actors analyze.intezer.com

lapsus$ Phishing supply chain telecom telecom industry Threat Intelligence Vermilion Strike