VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

# Creating Confidence Among Subscribers Faced with Growing Cyberthreats

A Technical Paper prepared for SCTE by:

**Bruce Van Nice**
Senior Product Marketing Manager
Akamai
Santa Clara, CA
650-575-4008
hvannice@akamai.com

# Table of Contents

**Title** **Page Number**

1. Introduction ... 3
2. Internet Users Face a Diverse Threat Landscape ... 3
3. The Road to Service Success ... 6
4. Keep it Simple ... 6
5. Complementing Other Security Services ... 7
6. Ensuring Transparency and Customer Control ... 7
7. Sourcing Threat Intelligence ... 8
8. Marketing to Ensure Success ... 9
9. Summary ... 10

Abbreviations ... 11

Bibliography & References ... 11

## List of Figures

**Title** **Page Number**

Figure 1 - Internet Crime Complaint Center (IC3) Internet Crime Report 2020 Summary of Complaints Received ... 4

Figure 2 - Internet Crime Complaint Center Internet Crime Report 2020 Summary of Types of Internet Crime Reported ... 5

Figure 3 - Graphical User Interface Showing Internet Activity and Impact of Web Filters and Various Kinds of Malicious Activity ... 8

 

# 1. Introduction

Today people depend on the Internet for just about everything: transacting, interacting, learning, traveling, and a multitude of other activities. The Internet also allows businesses of all sizes to reach new and larger markets and provides opportunities to work more efficiently by using digital tools that are increasingly economical and targeted at organizations with limited technical expertise. One of the downsides is theft of digital assets has become commonplace and for many organizations it represents a greater threat than physical theft.

Remote work challenges that began in 2020 continue as cybercriminals take advantage of elevated stress and unprecedented focus on topics related to the pandemic to maximize the value of their exploits. They saw a good opportunity to launch attacks and profit from dependence on the internet and technology. They used phishing and other kinds of internet-enabled fraud to target everyone from workers searching for personal protective equipment to families looking for information about help paying bills, and many others.

For ISPs there are opportunities to help subscribers navigate the always changing security landscape with new services that deter internet threats and are easy to use. This paper will talk about the product development process behind a security service targeted at Small Midsize Businesses (SMB) that was launched across a major North American cable network. It will:

Summarize the threats internet users face which motivated product teams to evaluate potential services

Outline a service strategy developed to help small and midsize businesses deter internet threats

Offer perspectives on the threat intelligence used to support the new security service

Discuss go to market to build awareness of security services and extend the value proposition of reliable high speed internet access

# 2. Internet Users Face a Diverse Threat Landscape

Cybersecurity is a visible topic today, news reports in mainstream media highlighting internet related crimes have become commonplace. The news is fueled by a multitude of organizations that track and analyze malicious activity - there's lots of data about cyber threats.

The US Federal Bureau of Investigation is a widely respected organization that runs the Internet Crime Complaint Center (IC3) whose mission is "to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity, and to develop effective alliances with industry partners."

The IC3 tabulates the data they receive and publishes it in the Internet Crime Report every year. The chart on the following page, copied from the 2020 report[1], summarizes the year over year trends from 2016 to 2020.

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

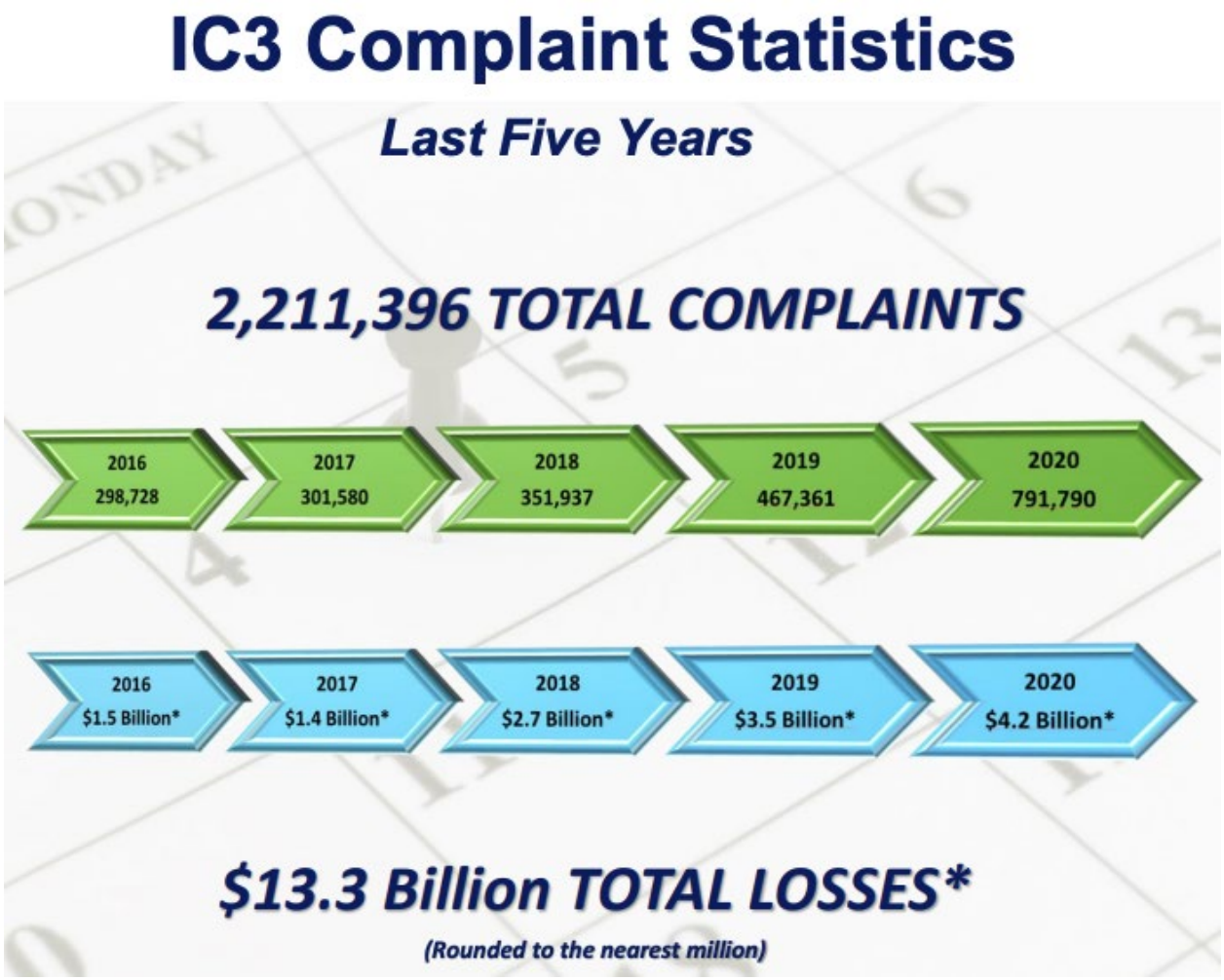


**Figure 1 - Internet Crime Complaint Center (IC3) Internet Crime Report 2020 Summary of Complaints Received**

The 791,790 complaints received from the American public in 2020 were a new record and represented a 69% increase over 2019. Reported losses exceeded $4.1 billion, a 20% increase over the previous year. The report also states: “These criminals used phishing, spoofing, extortion, and various types of Internet-enabled fraud to target the most vulnerable in our society - medical workers searching for personal protective equipment, families looking for information about stimulus checks to help pay bills, and many others. “

Another chart from the report summarizing threat vectors year over year is below. The 241,342 complaints tabulated for phishing scams more than doubled from 2019. To add color to the data and show how cyber criminals observe trends and tailor their exploits accordingly. The IC3 also received over 28,500 complaints about scams related to COVID-19.

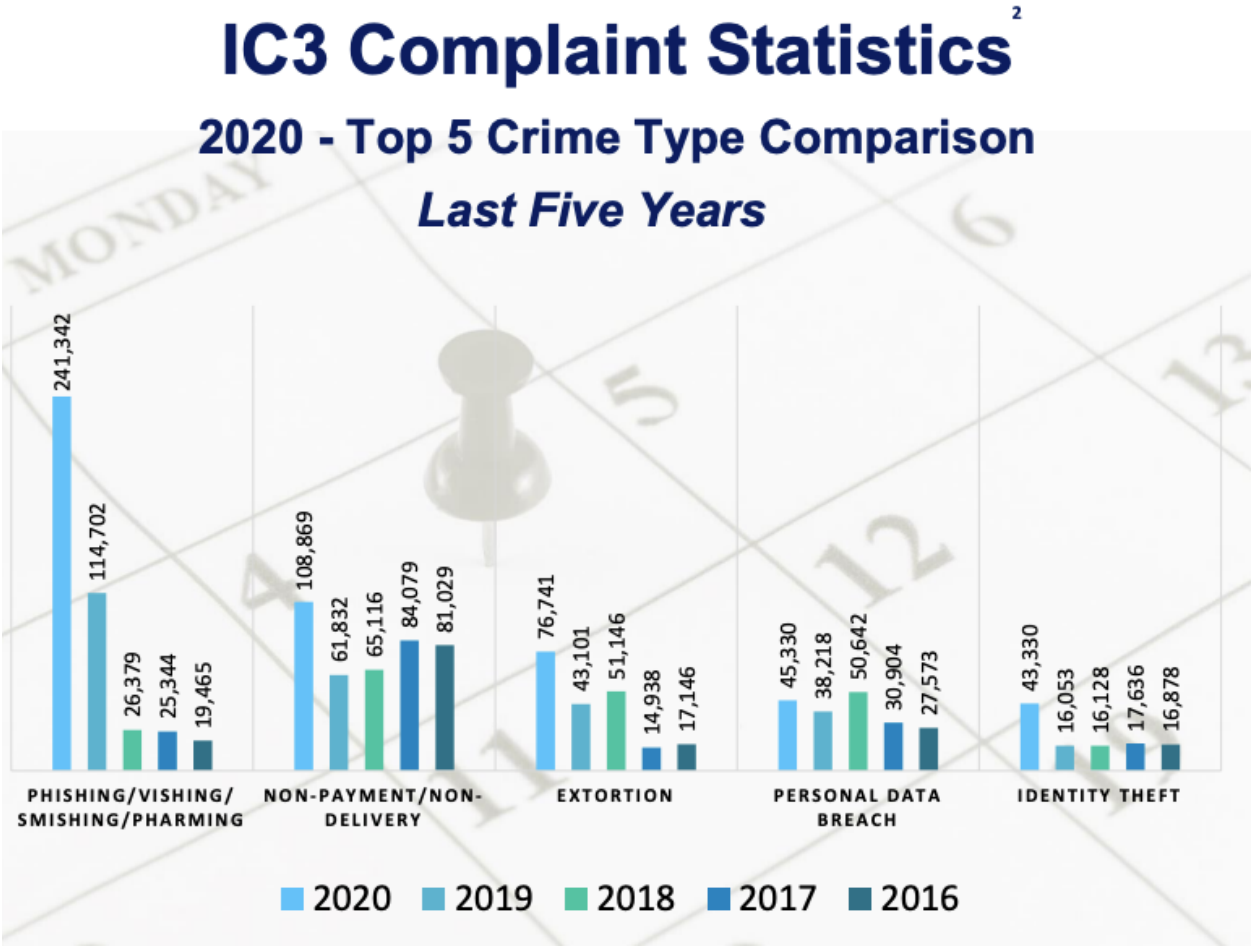


**Figure 2 - Internet Crime Complaint Center Internet Crime Report 2020 Summary of Types of Internet Crime Reported**

To add even more detail to this point, early in 2020 Akamai, a security company who participated in the development of the service covered in this paper, also showed a large amount of phishing activity focused on anything related to the pandemic[2]. The research showed hundreds of new COVID-related domains each day, most of which disappeared within 24 hours, which is consistent with longevity statistics they've historically gathered for names used for phishing.

Pandemic related scams are diminishing but hackers always innovate and find new themes to mine. Additional published research from Akamai shows a large increase in phishing prior to the holiday season last year[3]. Still more work discussed phishing campaigns modeled around cryptocurrencies and even Elon Musk[4]!

[2] https://blogs.akamai.com/2020/04/covid-19-phishing-exploiting-a-global-pandemic.html
[3] https://blogs.akamai.com/2021/02/phishing-holiday-season-attacks-on-the-rise.html
[4] https://blogs.akamai.com/2021/06/crypto-threats-surge-by-500-and-its-all-about-the-money.html

The point of these examples is not to offer a comprehensive overview of the threat landscape but to illustrate how hackers change their stripes to attract the attention of internet users and more importantly, get them to click on links and give up valuable data so they can make money. Diverse, fast changing exploits can make it hard for expert internet users to avoid being tricked, and it's even harder for average people.

## 3. The Road to Service Success

Like every company offering internet access services this organization was always looking for ways to improve their services. They were well known for performance and reliability and saw an opportunity to continue to contribute to online safety and help instill customer confidence with new security offerings.

The idea was to build on existing products which had embedded security features, like CPE for business customers with an integrated firewall and selectable levels of protection to control which kinds of protocol traffic are allowed or denied. Users can configure options to manage which protocol traffic will be permitted and blocked, like P2P applications.

More recently the team defined an optional DNS-based security service to defend workplaces against threats like malware, ransomware, phishing, botnets etc. The goal was to provide a foundational layer of defenses that take advantage of embedded network and operational strengths - such as scale, reach, reliability. This offering will be the focus of this paper.

In formulating product plans for this new service, initially targeted at Small and Midsize Businesses (SMB), several essential issues were considered to ensure success.

- Simplicity was paramount, surveys confirmed high awareness of cyberthreats but limited understanding of how to deter them - a service had to be simple to procure and operate.
- Complementing other security services was a critical consideration, most customers had security solutions and wanted to understand how anything new improved their posture
- Transparency was another requirement, subscribers had to be aware the service was operational, and what kinds of activity it was blocking.
- Customers had to have control and over time would expect even more "knobs and dials" to tune the experience

## 4. Keep it Simple

Large businesses are challenged dealing with internet security exposure but SMBs are even worse off because they may lack IT resources with specialized security expertise. A key product goal was to minimize the need for deep security expertise - with a model where the service "just works" after the service is activated (with some value add options discussed below) and covers all of the devices typically found in businesses today - PCs, phones, and even smart connected "things" like POS terminals, cameras etc. Other goals for the service included reducing installation overhead and ongoing maintenance - by eliminating software and hardware upgrades - as well as minimizing the expertise for configuring any optional features.

We provide every business subscriber with a graphical web portal that can be accessed anytime with a browser. The portal show's what's happening on their network and can be used to configure optional filters to manage what kinds of content is available on a workplace network, and what times certain websites are available to support Acceptable Use Policies.

## 5. Complementing Other Security Services

It was expected most business customers would already have security solutions and of course want to understand how anything new would improve their security posture. Examples of other services likely to be encountered include endpoint protection, specialized appliances, and "over the top" DNS-based filtering services. They considered how these options would shake out with respect to the planned service.

Endpoint software must be loaded on devices and requires ongoing maintenance, and it's not available for smart connected devices. Appliances offer protection but web traffic on the internet is increasingly encrypted and malicious activity can be completely invisible to security appliances, especially lower end models that don't have extremely sophisticated features to decrypt traffic (and experts to manage them). They also usually require periodic security expertise for ongoing care and feeding to be sure they operate properly. The user interface for security appliances is also typically aimed at someone with security knowledge, which an SMB may or may not have.

Security is about examining network traffic to determine whether it is malicious or legitimate. Approaches that operate in the data plane implement inline packet inspection to evaluate traffic. In the past it was possible to get visibility into most of the traffic on a network but the predominance of encryption has introduced significant limitations or complexity decrypting traffic. Inspecting packet traffic at line speeds has always been a costly operation, and inspecting encrypted traffic adds even more costs and operational overhead.

DNS filtering operates in the control plane. Incoming subscriber queries are matched against dynamic threat intelligence provisioned in resolvers, and policies can be applied to manage unwanted traffic. The team recognized attractive scaling capabilities since there is no need for pervasive monitoring and filtering of network traffic (and possibly decryption) and it can be layered on infrastructure already deployed and managed. Traffic from any device that makes DNS queries – the overwhelming majority – can be observed without the need for any client software. Threat coverage can be expanded by selectively forwarding suspicious traffic (typically domain names that point to both malicious and legitimate web resources) to proxies for further inspection. Experience has shown this is a small percentage of traffic, usually around 2%.

Based on these considerations DNS filtering was selected. The service is integrated with the subscriber internet access service (versus and off network "over the top" alternatives) to ensure performance and reliability.

## 6. Ensuring Transparency and Customer Control

Subscribers need a window into their service to understand how it is functioning. A portal user interface was specified to inform subscribers about their security posture and to allow them to configure other filtering features. Requirements included:

- Threat activity graphs showing threats blocked
- Configuration user interface for specifying web filters to support Acceptable Use Policies (AUP)
- Web filter graphs showing websites blocked by subscriber configured web filters
- Automated discovery of subscriber devices to support configuration of device-specific filters
- Subscriber-specified reports for archiving or offline analysis

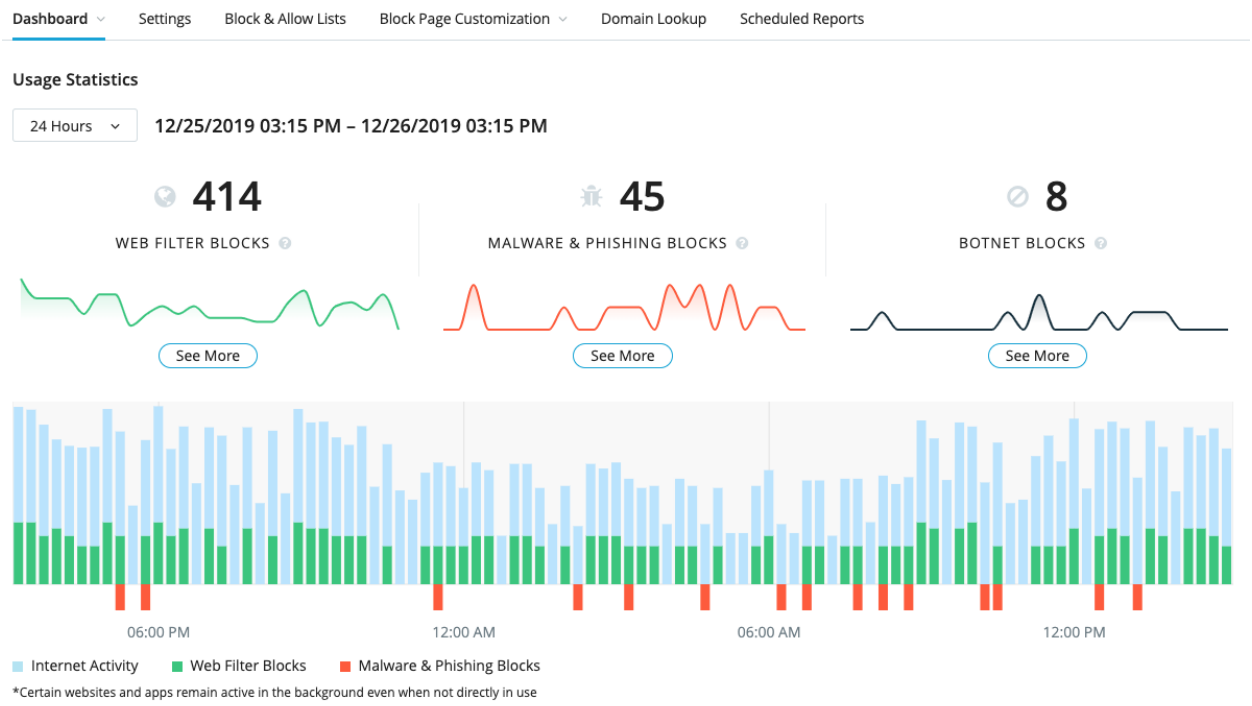


**Figure 3 - Graphical User Interface Showing Internet Activity and Impact of Web Filters and Various Kinds of Malicious Activity**

## 7. Sourcing Threat Intelligence

The value of security services is heavily influenced by the quality of the threat intelligence they employ. The threat landscape is incredibly diverse and it's simple for attackers to expose internet users everywhere to maximize the value of their efforts. Exploits also change quickly so attackers can stay ahead of security defenses that block their handiwork. For service providers in particular false positives can be extremely costly if subscriber access to favorite obscure websites is inadvertently blocked.

High level requirements for reconciling these objectives include:

- Large amounts of unencrypted raw data to maximize the coverage of increasingly sophisticated threats such as phishing, botnets and other kinds of malicious web resources
- High performance infrastructure to support near real-time processing of data to identify threats quickly and accurately to match the speed of change of today's exploits
- Machine learning algorithms that extend threat coverage by identifying subtle patterns and linkages in raw data that statistically match known threats used to train the algorithms
- Additional functions to validate threat entries are malicious to avoid blocking of legitimate web resources
- Software infrastructure to interconnect different processing systems so data flows among the "layers" in a structured way that allows inferences from one layer to the next

- Specialized processes to cull stale entries to keep threat lists from growing exponentially
- An iterative process to continuously refine, specialized algorithms that work together

Creating robust threat intelligence is complicated by the fact that some kinds of data is less available than in the past due to privacy regulations. More and more data is encrypted so it's opaque to analytical tools, and hackers increasingly use encryption to cover their tracks. Another advantage of DNS filtering is it overcomes these limitations. Unencrypted resolution data can be sourced from production resolvers or various kinds of network taps and anonymized to eliminate Personally Identifiable Information (PII).

DNS data has other useful characteristics for security research. Domain names and the Domain Name System (DNS) authorities and resolvers that support them, are fundamental to most security exploits. The DNS is widely used by malware developers because it connects everything on the internet from anywhere and virtually every network and device where an exploit might be activated will have access to the DNS. This means any device that emits a DNS query known to be associated with malicious activity can be identified as infected with the associated malware.

From a practical standpoint DNS queries are usually the first threat "signal" that's visible on a network where it can be detected remotely. Identifying activity at this stage is extremely useful as an exploit can potentially be disrupted before it does any real damage.

More details about how threat intelligence is developed can be found in a paper from SCTE 2018 "When Security and Privacy Collide New Approaches are Needed"

## 8. Marketing to Ensure Success

This is primarily a technical venue, but marketing is a critical part of any product launch process. Nothing sells itself anymore and building brand equity takes work - marketing investment helps ensure success. Product teams worked cooperatively with marketing to develop messaging that's aligned with other product and corporate marketing objectives.

For this service the marketing teams executed on a wide variety of initiatives. They built out a dedicated web presence in the commercial section of their website that provided all the information a prospective customer might be interested in. It highlighted all the major features of the service and offered complete descriptions of the value they offered to the intended customer base. Recognizing many potential customers were unlikely to be immersed in security jargon they used approachable language that was easy for typical SMB subscribers to understand. Other web pages present background information on security exposure so prospective customers can understand why protections are needed.

The marketing team also launched television advertisements across their US territory. Additional marketing campaigns reached customers directly with other media like email and marketing inserts as part of billing or other promotional packages.

There was additional effort for sales enablement. Teams were prepped on internet security basics so they could engage comfortably with prospective customers. They were equipped with simple product benefits they could convey and learned how to respond to questions about the service and how it compared with other security products prospects might already have. Business results

backed up the product development and marketing effort, with steady continuous growth in uptake.

## 9. Summary

Internet service providers everywhere are always looking for opportunities to improve their services. Speed and reliability aren't sufficient anymore. Awareness of security exposure on the internet creates an opportunity to contribute to online safety and help instill customer confidence with new security offerings. This DNS-based security service defends workplaces against threats like malware, ransomware, phishing, botnets etc., providing a foundational layer of defenses that take advantage of the power of network and operational strengths - scale, reach, reliability.

The product strategy for the new service considered several essential issues to ensure success:

- Simplicity was paramount because customers in the target segment often lack security expertise and specialized resources in general to oversee anything technically oriented
- It needed to complement other security services since most customers had security solutions and wanted to understand how anything new improved their posture
- Transparency was another requirement, subscribers had to be aware the service was operational, and what kinds of activity it was blocking.
- Customers had to have control and be able to tune the experience to match their business needs, preferences, and values

The new service was designed to complement other Small Medium Business (SMB) cybersecurity solutions such as firewalls and anti-virus. It adds threat defenses backed by machine learning algorithms that process live streamed DNS data in near real time to uncover new malicious activity quickly and accurately. Customized web content filters allow business managers to enable "Acceptable Use Policies" to manage the kinds of web content that are accessible on workplace networks. Investments in marketing and sales enablement were made to ensure good penetration of the service and attainment of business goals.

# Abbreviations

| | |
|---|---|
| CPE | Customer Premises Equipment |
| DNS | Domain Name System |
| FBI | Federal Bureau of Investigation |
| IC3 | Internet Crime Complaint Center |
| ISP | Internet Service Provider |
| P2P | Peer to Peer |
| PII | Personally Identifiable Information |
| SMB | Small and Midsize Business |

# Bibliography & References

1. Federal Bureau of Investigation Internet Crime Complaint Center Internet Crime Report 2020 https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
2. The Akamai Blog *Exploiting a Global Pandemic* Bruce Van Nice https://blogs.akamai.com/2020/04/covid-19-phishing-exploiting-a-global-pandemic.html
3. The Akamai Blog *Phishing Holiday Season Attacks on the Rise* Or Katz https://blogs.akamai.com/2021/02/phishing-holiday-season-attacks-on-the-rise.html
4. The Akamai Blog *Crypto Threats Surge by 500% and it's All About The Money* Or Katz https://blogs.akamai.com/2021/06/crypto-threats-surge-by-500-and-its-all-about-the-money.html