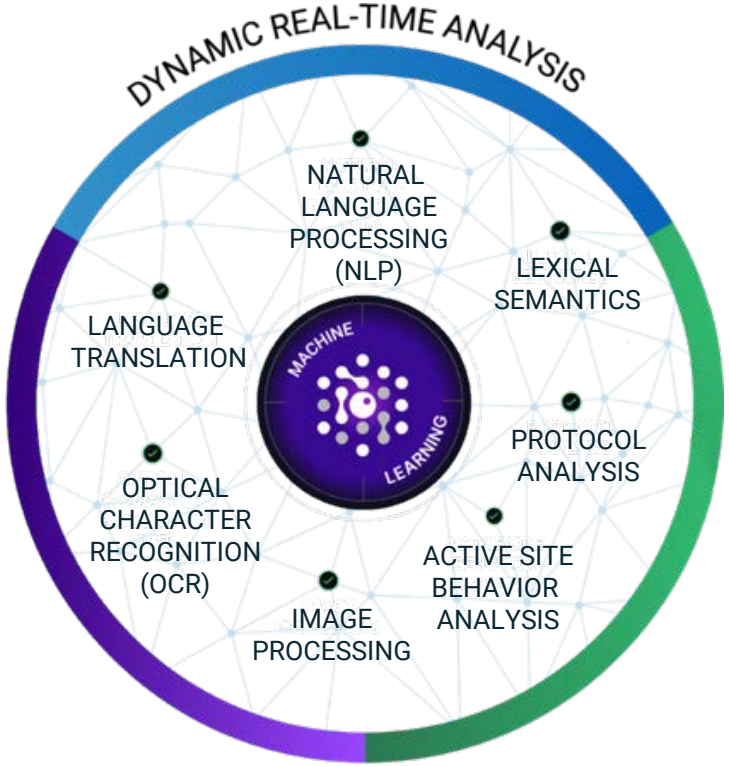

# Phishing 2.0 Threat Email and Firewall Analysis

# SlashNext Assessment Overview

- The analysis detailed within this presentation has sent 30-days of your email and network traffic through the SlashNext engine in order to expose the gaps in your existing coverage and to identify the protection that SlashNext can bring to your organization.




SEER™ AI Detection Engine

SLASHNEXT

# Firewall Threat Victimization

Dates Analyzed: 12-1-2020 to 12-30-2020 (30-days)

- The analysis of your Palo Alto Networks firewall log for the 30-day period shows that 14% of your users fell victim to 308 total phishing attacks.
- The threats identified here indicate what all other existing defenses have overlooked.
- This analysis is done only against the traffic that traversed the firewall, any at-home users or mobile users are not covered by this analysis, if these other users are considered the true victimization would be at least 2.5x greater.

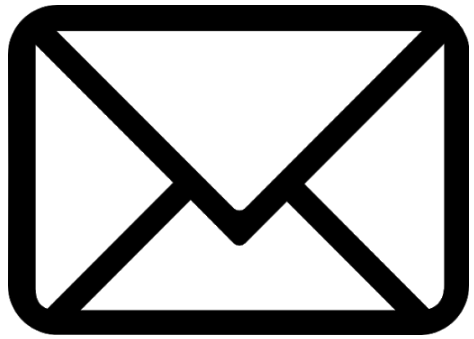
| 14% | 308 |
|---|---|
| Users Victimized | Threats Executed |
| 1,102 | 10,967,154 |
| IPs Identified | Transactions |
| 154 | 2 |
| IPs Victimized | Average Threats Per Victimized IP |

SLASHNEXT

# Email Threat Exposure

Dates Analyzed: 12-1-2020 to 12-30-2020 (30-days)

- The analysis of your Office 365 email messages for the 30-day period shows that 80% of your users were exposed to threats and that a total of 9,456 total threats were delivered to inboxes.
- This analysis is done against the Office 365 service only, as a result it demonstrates what any pre-email defenses, like a SEG (Secure Email Gateway) overlooked.
- This assessment only considers corporate email, if personal user email is also considered the total threat exposure would be at least 2x greater.



| 80% | 9,456 |
|---|---|
| Users Exposed | Threats Identified |
| 985 | 2,068,500 |
| Users Identified | Messages Scanned |
| 788 | 12 |
| Users Threatened | Average Threats Per User |

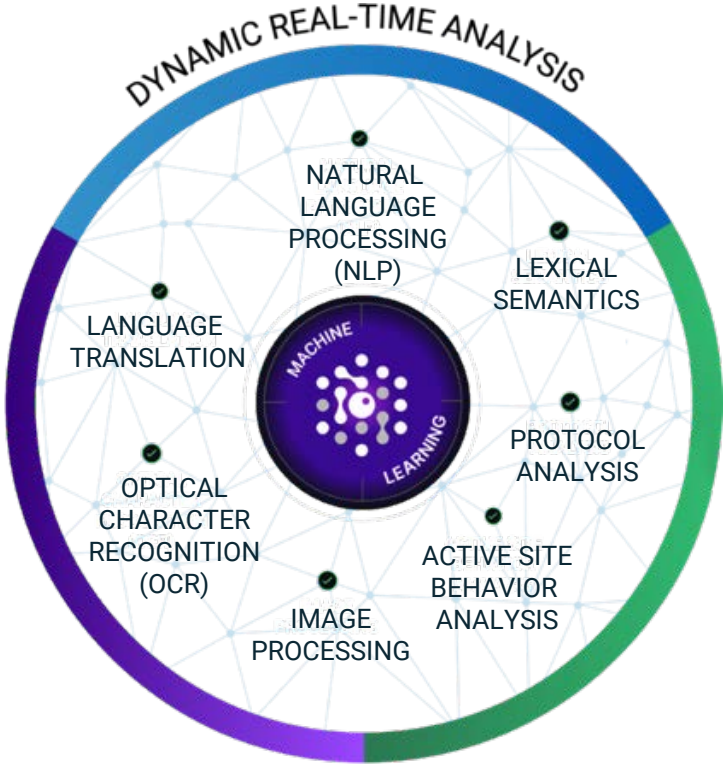
SLASHNEXT

# SlashNext Overview

- Phishing is the #1 threat facing organizations today.
- SlashNext is a company solely dedicated to eradicating phishing in order to stop criminals and to protect organizations and their users.
- The SlashNext solution is an AI based Phishing 2.0 Defense offering the highest level of protection against 0-day phishing threats.

# SlashNext Overview

- The solution leverages a patented phishing “sandbox” engine where threats are opened in real browsers and a full and exhaustive analysis and categorization happens using our AI, ML Vision and NLP engines so that threats can be identified and detonated before users are exposed.
- The engine produces the worlds largest phishing intelligence, with a measured efficacy rate higher than 99% and a false positive rate less than 1-in-1Million

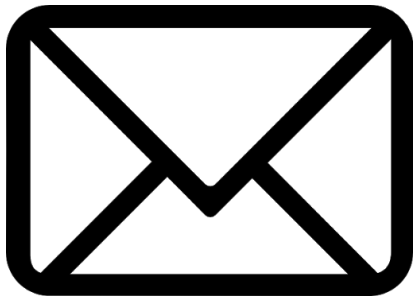



SEER™ AI Detection Engine

SLASHNEXT

# Assessment Parameters

- Total Users:  985
- Email Service:  Office 365
  - Dates Analyzed:  12-1-2020 to 12-30-2020
  - Report Days:  30
- Firewall:  Palo Alto Networks
  - Dates Analyzed:  12-1-2020 to 12-30-2020
  - Report Days:  30
- Notes
  - This assessment represents only the traffic that flows via the corporate network, home users and mobile users are not represented.



SLASHNEXT

# Total Threat Breakdown by Type

| Type | Email | Firewall |
|---|---|---|
| Phishing | 6,947 | 154 |
| Scareware | 1,082 | 49 |
| Rogueware | 1,133 | 65 |
| Scams | 294 | 32 |
| Data Exfiltration | 0 | 9 |
| **Total** | **9,456** | **309** |

The table above represents the break down, by type, of threats users were exposed to via email and the threats users were feel victim to as identified by the firewall log.

SLASHNEXT

# Phishing/Credential Stealing

| Type | Email | Firewall |
|---|---|---|
| Phishing | 6,947 | 154 |

Estimated Risk Per Incident: up to $400[1]
Total Risk Identified in 30-days: $61,600

Credential Stealing is one of the oldest form of Phishing. This type of attack tricks the user into giving up their credentials by representing a near-copy of a legitimate web page. Replica pages often leverage popular global brands such as Google, Microsoft, Dropbox, and Yahoo for credential stealing attacks. Some come complete with functional "Password Reset" options, and some ask for secondary email accounts, mobile phone numbers, or security questions for "enhanced security".

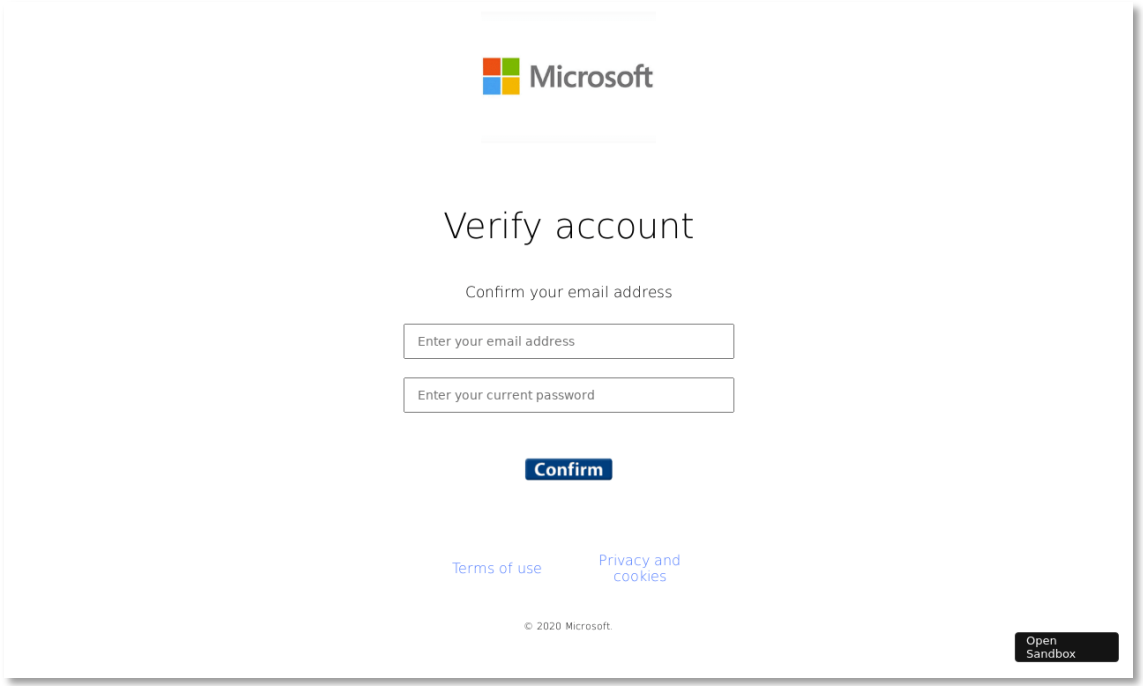
These attacks are effective because the user usually can't differentiate between the fake and legitimate page. Virtually any brand can be easily impersonated, and the inherent trust that the brand has created with its customers is the very thing that attackers use to their advantage. Enterprises have tried to reduce their risk to these sorts of attacks by training their employees on how to identify and avoid these kinds of fake sign-in pop ups and pages. However, despite training, humans make mistakes.

1: https://smallbiztrends.com/2019/07/phishing-statistics.html

SLASHNEXT

# Phishing/Credential Stealing Example

| Threat Status | Active |
|---|---|
| “Virus Total”[1] Detections | 0 |
| Date First Seen | 12-10-2020 |
| Present in User Emails | 197 |
| Clicked by IP Addresses | 3 |
| hxxps://s7g0l[.]csb[.]app | |




1: Virus Total is a service managed by Google where results can be compared to 86 other anti-phishing solutions. These results have been compared to the other vendors participating in Virus Total

SLASHNEXT

# Scareware

| Type | Email | Firewall |
|---|---|---|
| Scareware | 1,082 | 49 |

Estimated Risk Per Incident: up to $2.4M[1]

This alert indicates that a user is trying to visit a malicious web site setup for conducting technical support scams. Technical support scams use scare tactics to trick gullible victims into believing that their computer has either crashed or that a virus has been detected on their computer. These scams try to lure victims into calling a fake technical support hotline which, if successful, can lead to telephone fraud. The goal is usually to gain remote access to the system and collecting sensitive user information. These scammers may also ask their victims to pay for their fake support.

Once connected, agents may:
1) Install malware for remote access or data exfiltration;
2) Disable endpoint protection or re-configure them to whitelist, trust or ignore tools that these scammers may want to use.

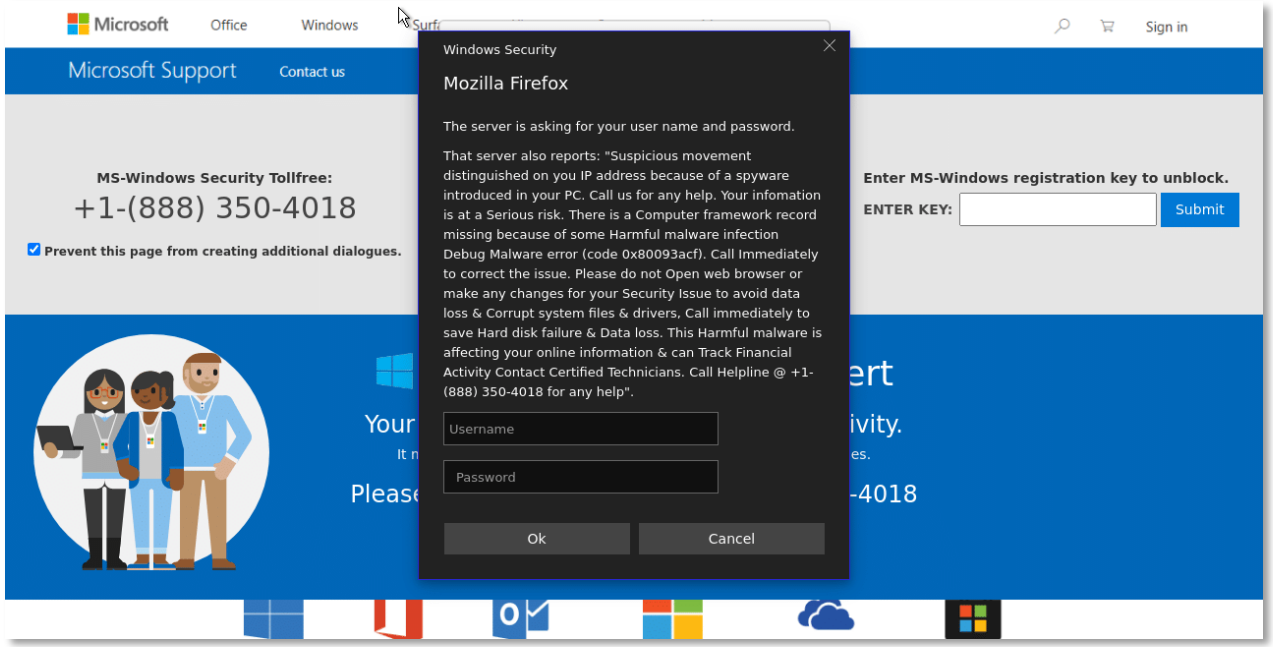
Remote Access apps like TeamViewer, and LogMeIn, are also used as part of tech support scams. These legitimate apps allow the scammer to access the victim's computer and install malware such as keyloggers or backdoor right under the unsuspecting victim's nose

1: https://smallbiztrends.com/2019/07/phishing-statistics.html

SLASHNEXT

# Scareware Example

| Threat Status | Active |
|---|---|
| “Virus Total”[1] Detections | 0 |
| Date First Seen | 12-10-2020 |
| Present in User Emails | 16 |
| Clicked by IP Addresses | 2 |
| hxxp://159[.]89[.]195[.]129/schoolstudy/forlearning/FFfdfd888247ucode0xhelpms888/index.php | |




1: Virus Total is a service managed by Google where results can be compared to 86 other anti-phishing solutions. These results have been compared to the other vendors participating in Virus Total

SLASHNEXT

# Rogueware

| Type | Email | Firewall |
|---|---|---|
| Rogueware | 1,133 | 65 |

Estimated Risk Per Incident: up to $2.4M[1]

These type of Social Engineering and Phishing attacks usually trick users in downloading fake system cleaners or anti-virus tools by showing fake infections or malware activities on their system. In some case, these types of attacks lure their victims into installing malicious videos players or rogue browser extensions with the intent of giving users some promised interesting/useful functionality.

These attacks fundamentally try to exploit the users trust in global brands with the end goal of getting them to wittingly (or unwittingly) permit socially engineered malware to get onto his or her system.

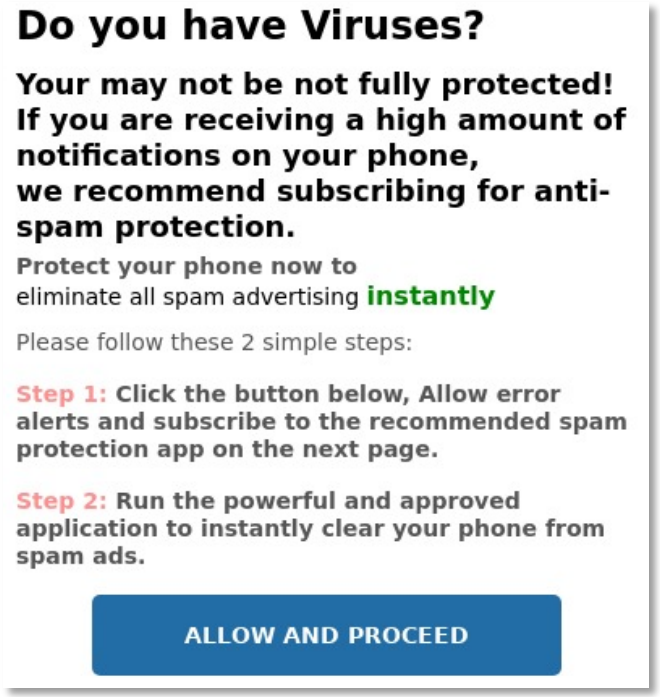
Common malicious characteristics include:
1. Snooping on active browser sessions to perform unauthorized actions such as sniffing a user's credentials from memory.
2. Actively parsing web page content ("Man in the Browser").
3. Launching third-party Phishing pages within browser windows.
4. Hijacking search queries and results and selling it to third-party affiliates.

1: https://smallbiztrends.com/2019/07/phishing-statistics.html

SLASHNEXT

# Rogueware Example

| Threat Status | Active |
|---|---|
| “Virus Total”[1] Detections | 0 |
| Date First Seen | 12-18-2020 |
| Present in User Emails | 15 |
| Clicked by IP Addresses | 2 |
| hxxps://70[.]gadget-errors3[.]com/0203-av-cmpl-wh/ | |




1: Virus Total is a service managed by Google where results can be compared to 86 other anti-phishing solutions. These results have been compared to the other vendors participating in Virus Total

SLASHNEXT

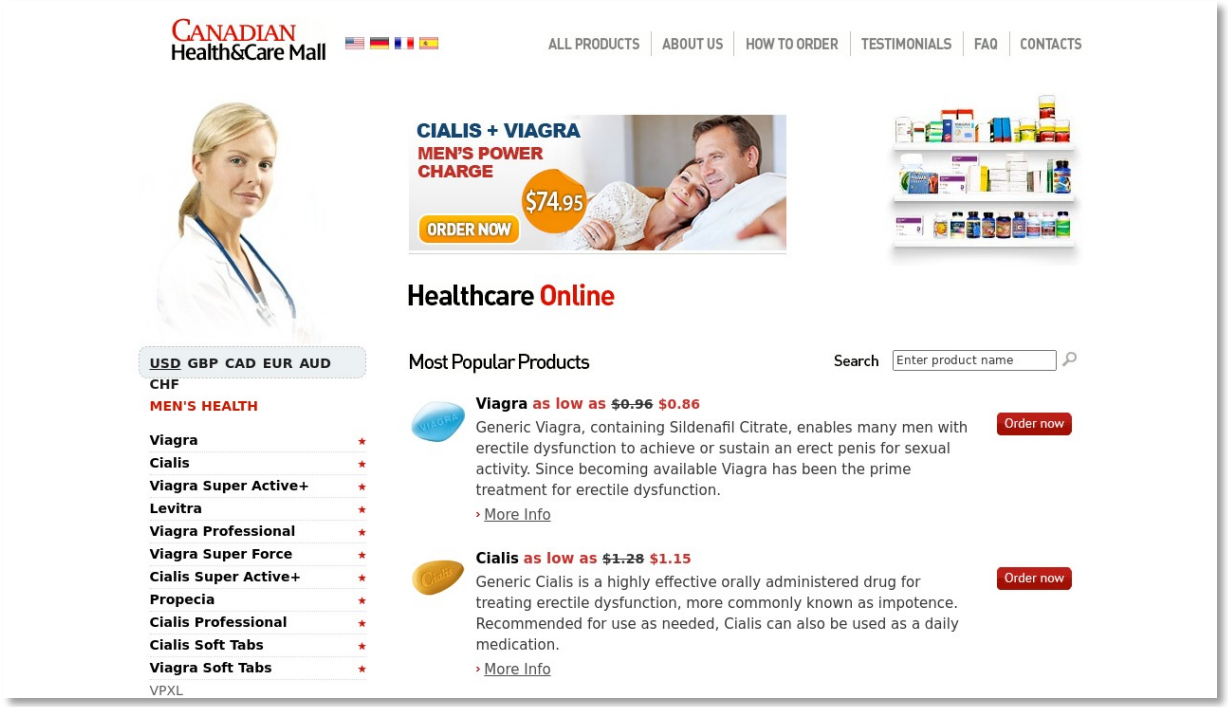
# Scams

| Type | Email | Firewall |
|---|---|---|
| Scams | 294 | 32 |

This alert indicates that a user is trying to visit a fraudulent web site. These Internet Scams are a type of social engineering attacks that create a sense of excitement for their victims and ask them for sensitive information in order to claim a reward or with a promise of an interesting video. In some case these Web sites have been observed serving counterfeit products on low prices as part of a Credit Card fraud scheme.

# Scams Example

| Threat Status | Active |
|---|---|
| “Virus Total”[1] Detections | 0 |
| Date First Seen | 12-07-2020 |
| Present in User Emails | 5 |
| Clicked by IP Addresses | 2 |
| hxxp://gocemitrevski[.]xn--h1ahfb6bh[.]xn--p1ai | |




1: Virus Total is a service managed by Google where results can be compared to 86 other anti-phishing solutions. These results have been compared to the other vendors participating in Virus Total

SLASHNEXT

# Data Exfiltration/Callback

| Type | Email | Firewall |
|---|---|---|
| Data Exfiltration | 0 | 9 |

Data exfiltration occurs when malware and/or a malicious actor carries out an unauthorized data transfer from a computer. It is also commonly called data extrusion or data exportation. Data exfiltration is also considered a form of data theft.

1: https://smallbiztrends.com/2019/07/phishing-statistics.html

SLASHNEXT

# Summary

Stop the #1 threat with the #1 solution


- The SlashNext solution identified 9,764 threats that were un-identified by your existing defenses.
- 80% of your email users are exposed to a threat every 2 days.
- 14% of your users are victimized by threats monthly.

Total Annual Risk From Credential Stealing Alone $739,200

The SlashNext 2.0 AI Phishing Platform is the only solution capable of addressing all 0-day phishing threats across all payloads via all communication channels.

SLASHNEXT