Attackers in a Remote Work World

Justin Gilbert
Senior Channel Marketing Director

Agenda

1. Shift in Remote Work
2. Evolving Threat Landscape
3. Security Simplified
4. Prevent & Detect Threats with Ease

zix | appriver

Remote Work

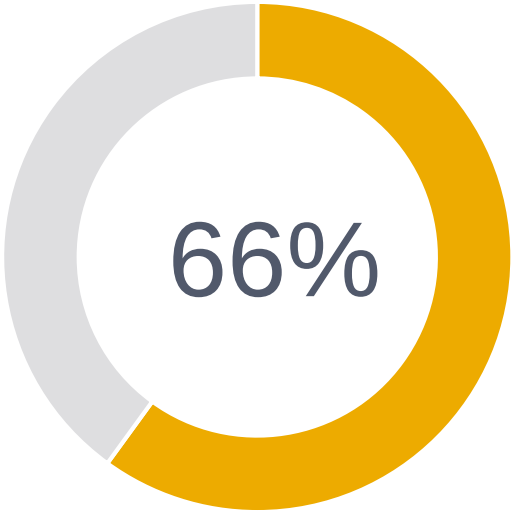
Trends in Hybrid and Remote Work

Let’s hear from you and what you’re seeing trend in your organization.

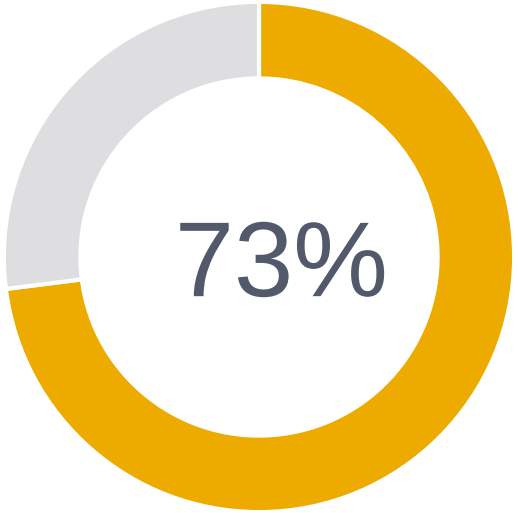
- What are you doing to adapt to a more remote workforce?
- What security measures have you taken to ensure your organization remain secure?

zix | appriver

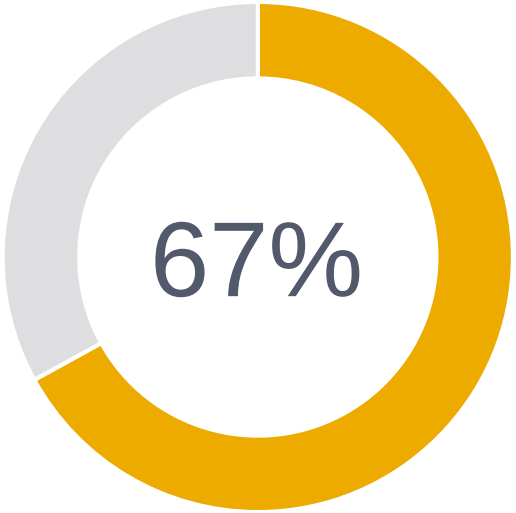
Trends in Hybrid and Remote Work



Of leaders say their company is considering redesigning office space for hybrid work



Of employees want flexible remote work options to stay



Of employees want more in-person work or collaboration post-pandemic

Threat Landscape

Data Driven Security Solutions

206M
Attached Malware Attacks stopped

7.4B
Social Engineering Attempts Blocked

$26B+
Global BEC Losses

24/7 Team of Security Analysts that:

- Identifies threats and vulnerabilities
- Creates rules and evolves defense to changing threatscapes

Threat detection powered by 18 years of experience, technology and innovation

- Our Security Operations Center is always busy and…
- Our Email Security is always evolving to defend against the latest (and upcoming) threats.

zix | appriver

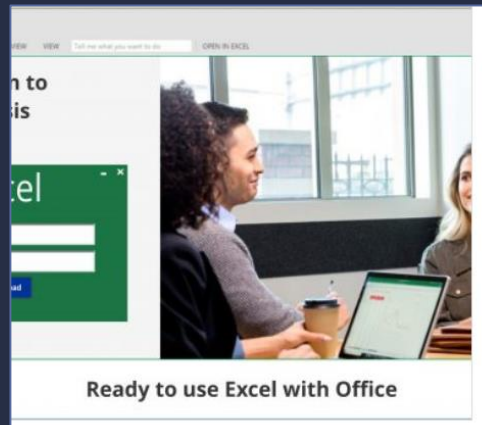
Solarwinds Supply Chain Attack

SUNBURST wasn't the only malware that factored into the SolarWinds supply chain attack. Several other distinct digital threats factored into the infection flow:

- **TEARDROP and BEACON:** FireEye found at least one SUNBRUST instance that delivered a previously unidentified memory-only dropper called "TEARDROP." The attackers used the resource to execute a customized Cobalt Strike BEACON.
- **SUNSPOT:** In mid-January, CrowdStrike learned that the SolarWinds supply chain attackers had used SUNSPOT to insert the SUNBURST backdoor into the software builds of SolarWinds' Orion IT management platform. This malware came equipped with several safeguards to prevent the Orion safeguards from failing and to thereby prevent the attackers from learning of the adversaries' presence.
- **RAINDROP:** It was just a week later when Symantec uncovered RAINDROP, a loader which like TEARDROP delivered the Cobalt Strike payload. The resource was a bit different, however, in that it didn't rely on the SUNBURST backdoor for distribution. Instead, it appeared on networks where attackers had already compromised at least one computer with SUNBURST.

Hafnium – Microsoft Zero-Day Attack

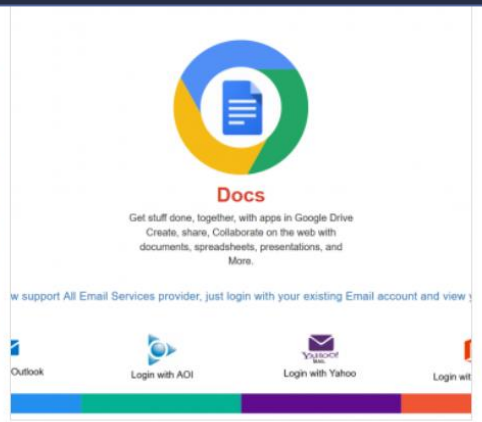
Phishing Kits For Sale



Excel scam page style 3

~~$90.00~~ $80.00

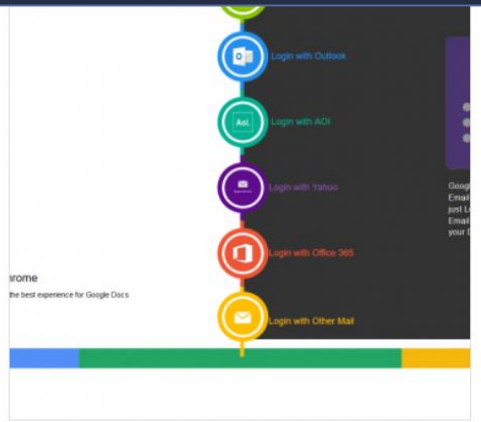
ADD TO CART



GoogleDoc scam page style 1

~~$90.00~~ $80.00

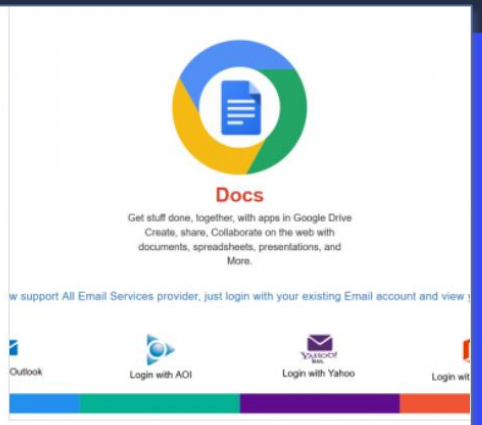
ADD TO CART



GoogleDoc scam page style 2

~~$90.00~~ $80.00

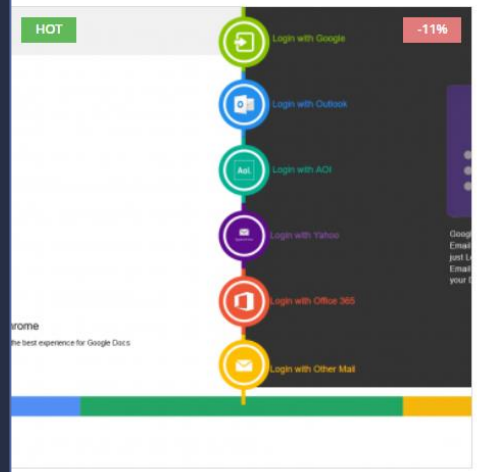
ADD TO CART



Googledoc scam page style 4

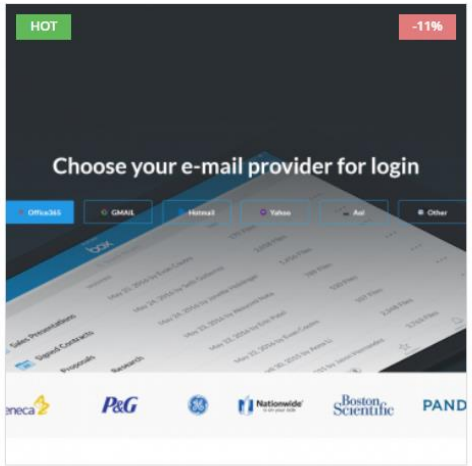
~~$90.00~~ $80.00

ADD TO CART



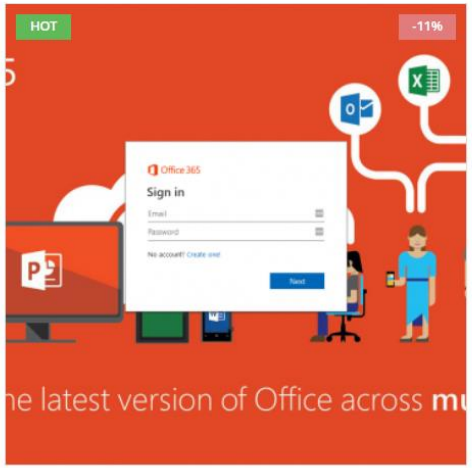
Googledoc scam page style 5

~~$90.00~~ $80.00



Office Email 365 Scam Page Style 7

~~$90.00~~ $80.00



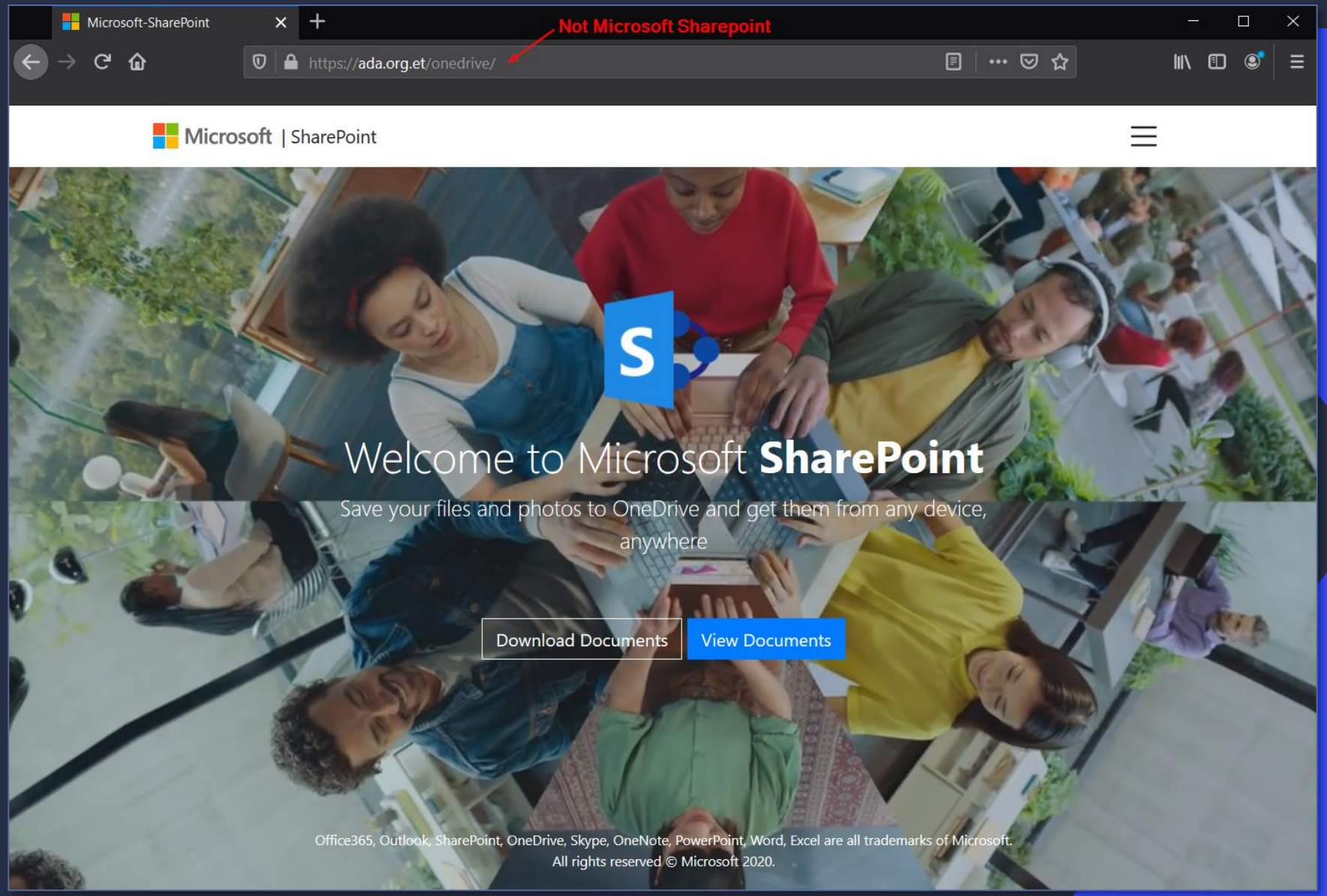
Office Email 365 Scam Page Style 8

~~$90.00~~ $80.00

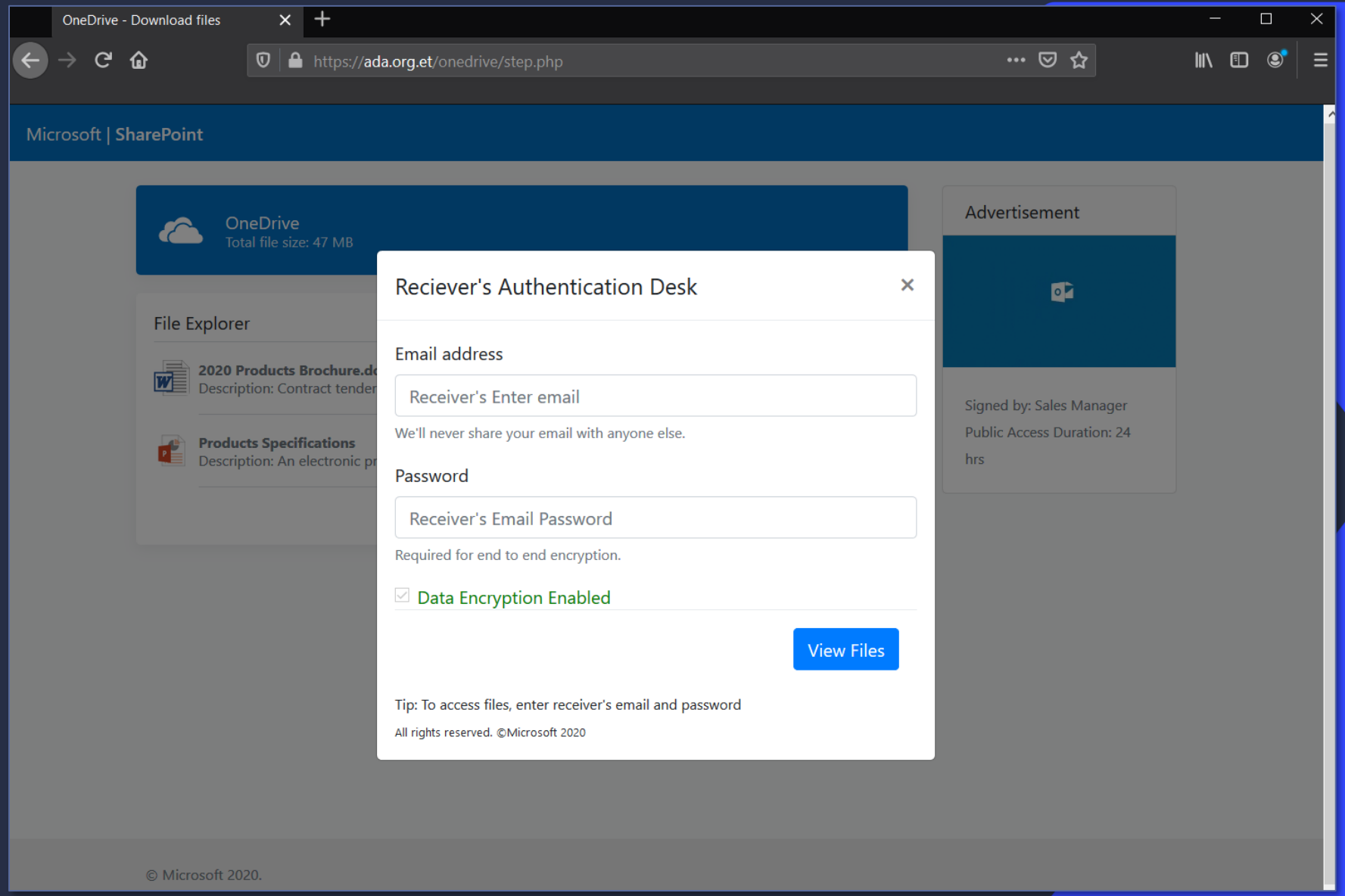
Office Share Point Style 1

~~$90.00~~ $80.00

Phishing Kit Example



Goal - Credential Harvesting



COVID19 Malware Example – jRAT / Adwind

From Candice <info.mmd@[redacted].com>
Subject **Purchase Order (PO For-COVID-19 Products)**
To info@[redacted].ch

Reply | Reply All | Forward | More

1:57 AM

Kindly find Attached PO and below items and advise if you can provide us a quote for it.

1-Latex examination gloves : Free powder NON-Sterile QTY 6,000,000 (six Million only)

SIZE: Medium with MOH wight with protein

Content: Less than 50 UG

ISO 1193: Printed in box

(All specifications same as in offer)

Packing : 100 PCS/PKT & 10 PKTS/CASE

2-Examination free powder latex gloves have excellent tactile sensitivity , made with high quality natural rubber QTY 10,000,000 (Ten Million only)

Latex for strength, Disposable

NON-Sterile

SIZE: Large

Packed : 100 PCS/PKT

3- Gown yellow – fluid repellent (plastic) QTY 1,000,000 (One Million only)

Type: Front splash proof , breathable back ,10 Pieces in a bag .

Properties :Fluid repellent -front , breathable back , Easy tear free, Knitted elastic cuff in hands

Color: yellow.

Dimensions : X large- Width 1400 MMX ,Length 1600 MM

Package: Boxes inside a plastic bag covered with transport carton

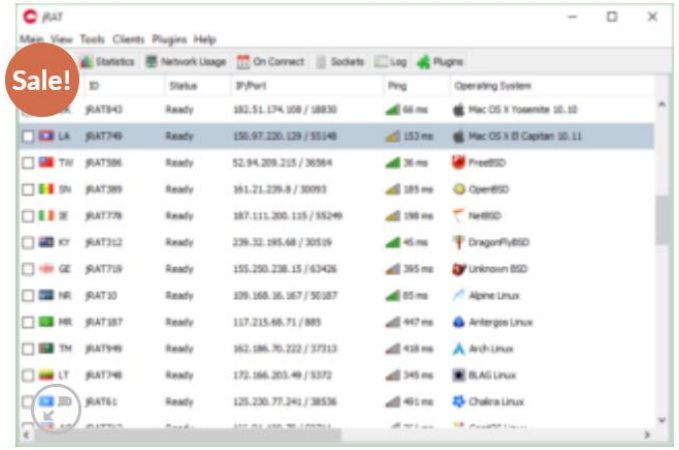
Thanks

Best regards

Adwind/jRAT

1 attachment: PO For-COVID-19 Products.jar 588 KB

Save



HOME / SOFTWARE / REMOTE ADMINISTRATION TOOLS

jRAT Java 6.0.0-rc.1

~~$35.00~~ **$30.00**

Important: You will receive three versions The Latest version 6.0.0-rc.1 – 6.0.0-beta.1 and 5.5.2

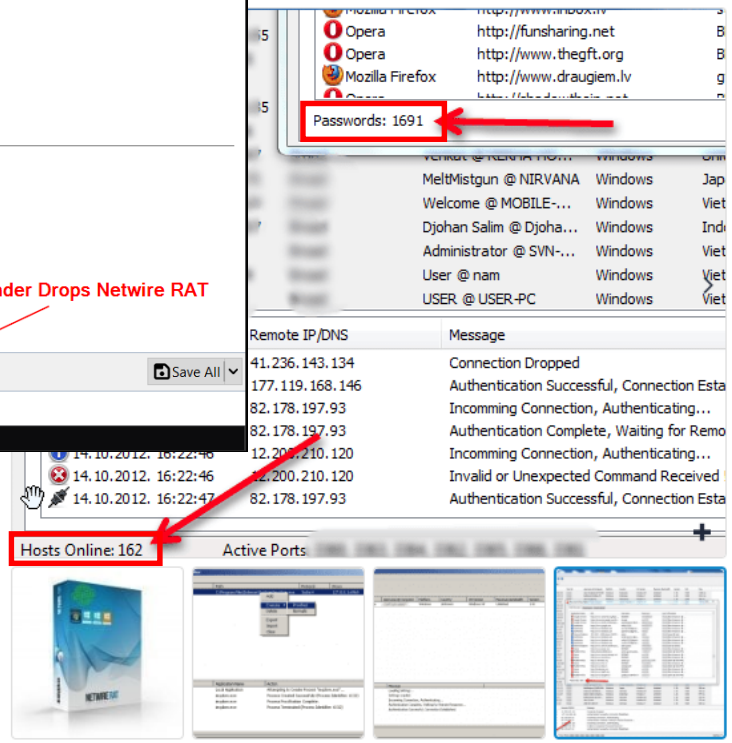
jRAT is a Java Remote Administration Tool with a clean native interface and multi-platform controller and client.

jRAT is fitted with all the tools to take you from being a doubtful employer or curious parent to being the real administrator of your intellectual property. OSCelestial is perfect for any use, business environment as the only precursor required is Java.

- Extremely stable
- Customizable
- Multi-OS RAT
- GUI compatible with any OS
- Keylogger

- 1 + ADD TO CART

COVID19 Malware Example – GULoader/Netwire



NetWire RAT

(There are no reviews yet.)

$180.00

Accessibility:

Connect to your Windows, Linux, Mac OS X servers, workstations, desktops, laptops and Android Smartphones from any place provided the Internet or Network access is available. NetWire can be customized to suit your daily needs, such as remote support, live forensics or even monitoring your children at home.

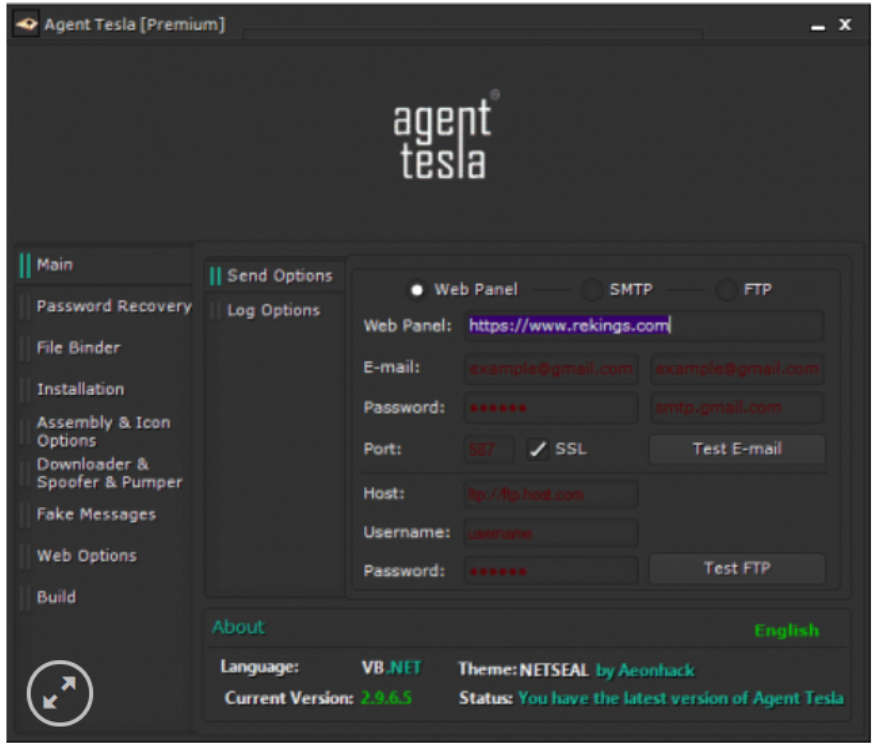
- Very stable
- No dependencies
- Use to-use gui
- Remote Desktop
- Webcam Spy
- Remote file execution

Categories: Remote Administration Tools, Software

1 ADD TO CART Add to Wishlist

SHARE

AgentTesla Advertisement






HOME / SOFTWARE / KEYLOGGERS

Agent Tesla

$20.00 – $100.00

Agent Tesla Keylogger supports UTF-8

DESCRIPTION ADDITIONAL INFORMATION REVIEWS (0)

Agent Tesla is modern powerful keystroke logger. It provides monitoring your personal computer via keyboard and screenshot. Keyboard, screenshot and registered passwords are sent in the log.

- Stable
- Unicode Support
- Multi-language Support
- Fast & Stable
- Password Recovery (Chrome, Firefox, IE, Yandex, Opera and more..)
- Different Delivery (PHP, SMTP, and FTP.)
- Encrypted and clean logs
- Supports All Email Providers

Supports email, Support FTP, Web panel, Windows startup, Startup Persistence, Process Protection, Advanced Keystroke Monitoring, Clipboard Logger, IP logger, Advanced password recovery and more.

Packages: 6 months

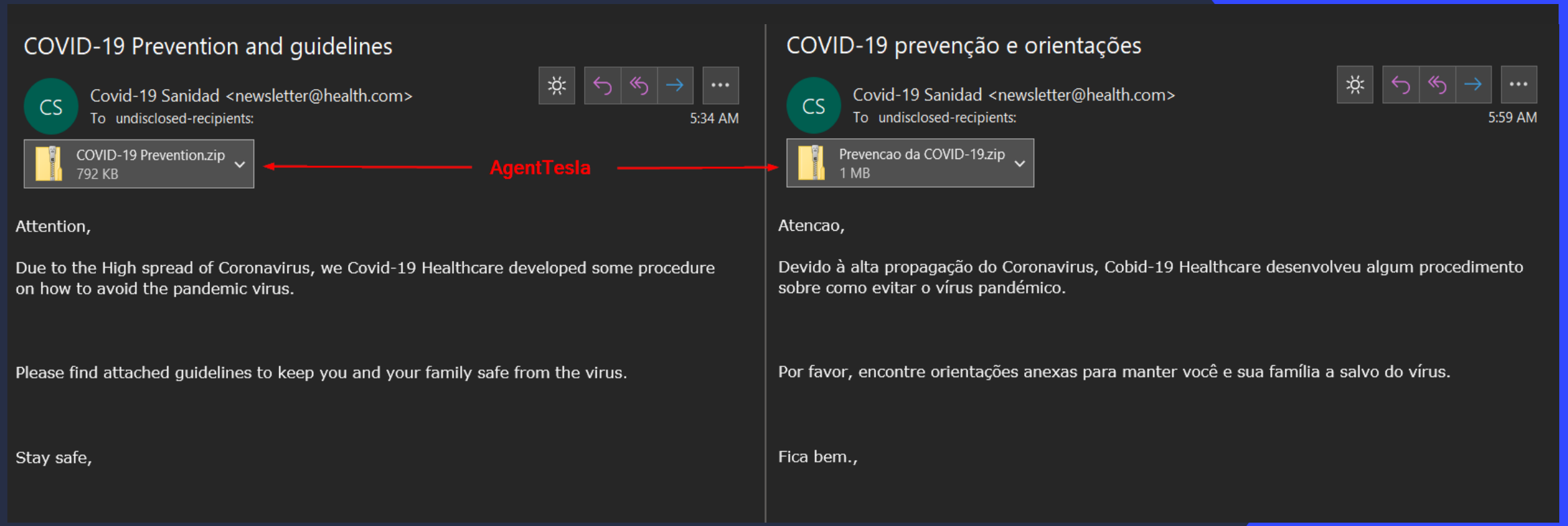
Choose an option
1 month
3 months
6 months
Lifetime

$65.00

\- 1 +

ADD TO CART

COVID19 Malware Example – AgentTesla



COVID19 Malware Example – Dridex

Preparing businesses and employer's work areas for a coronavirus (Covid-19) outbreak prevention

JF

Juanita Franco <gonzalez.josephggqk@wp.pl>

To [redacted]@[redacted].co.uk

Reply | Reply All | Forward | ...

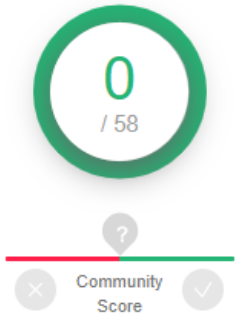
Fri 4/10/2020 9:35 AM

Email Address Doesn't Match Name

Direction 5613.xls
195 KB

Business and employer work areas Coronavirus spread avoidance information
Check the attachment!

Best Wishes, Dr. Juanita Franco



No engines detected this file

d36a1b70237335b445b5a7fa69c24909a5710a427e145fcf247fd3fc5588cf16

Direction 5613.xls

xls

194.50 KB
Size

2020-04-10 22:11:44 UTC
a moment ago

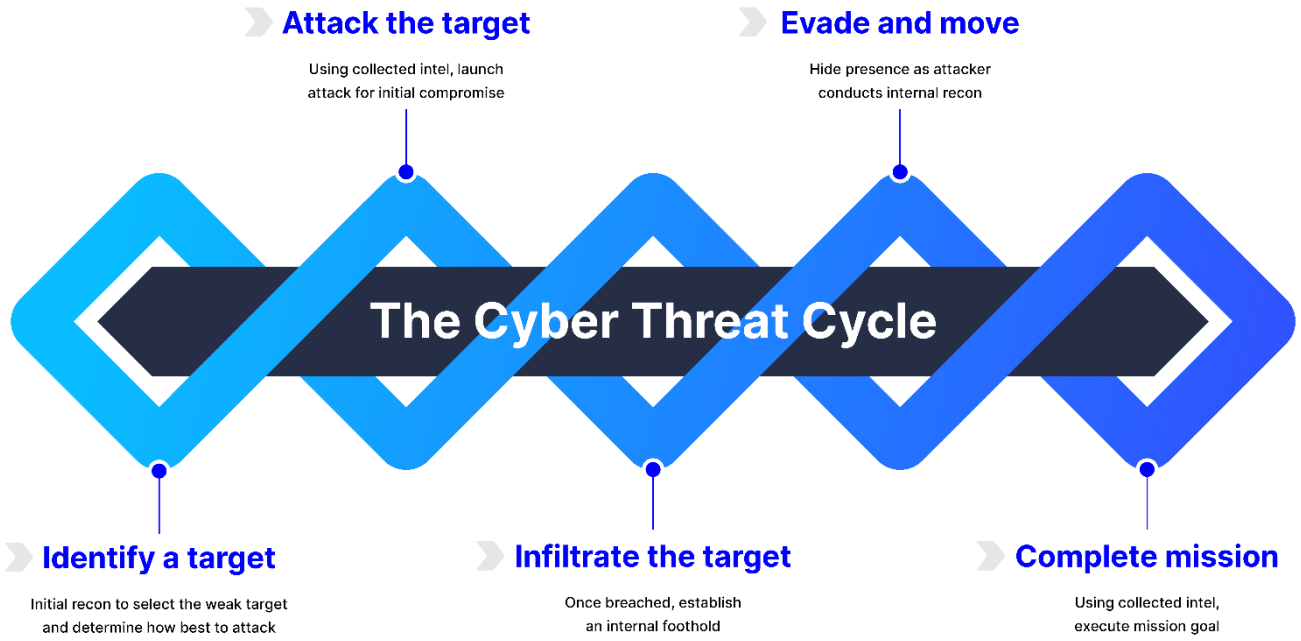
XLS

Security Simplified

zix | appriver

How to Address the Challenges

Threats are more than just the headline

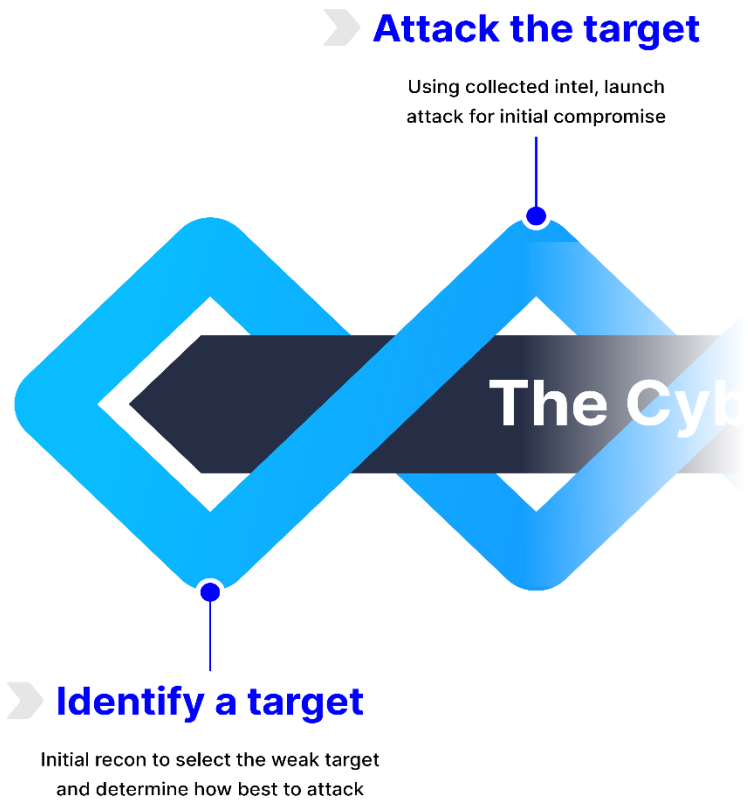


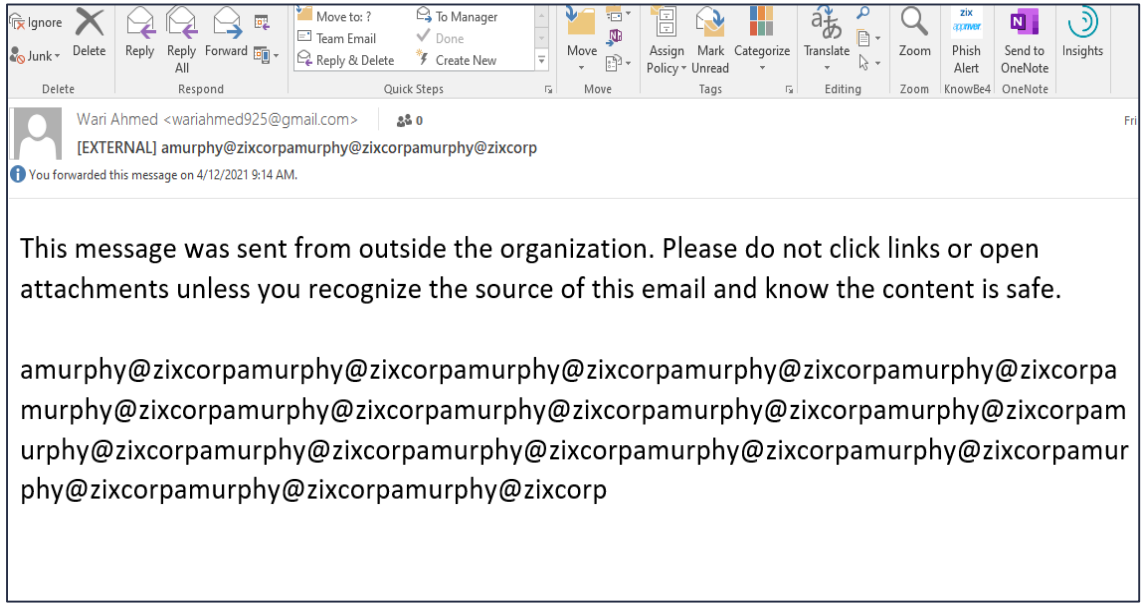
Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China

The hackers started their attack in January but escalated their efforts in recent weeks, security experts say. Business and government agencies were affected.

An Opportunity to Talk About the Challenge

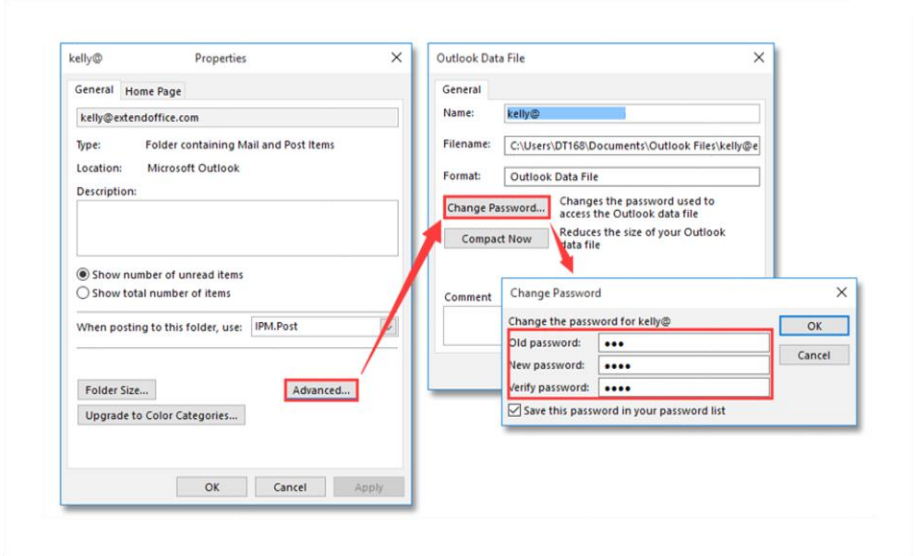
Email is the vector for Recon & Attack

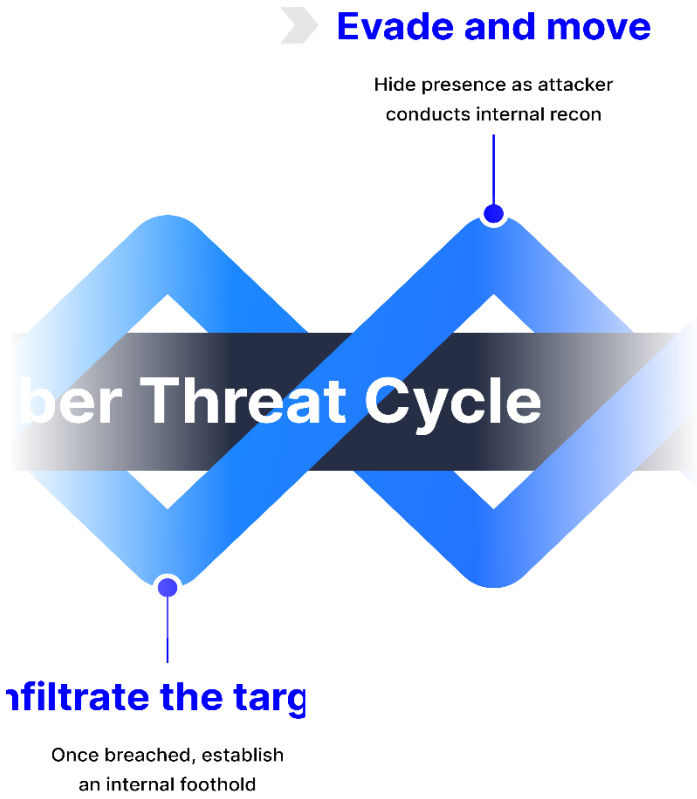




An Opportunity to Talk About the Challenge

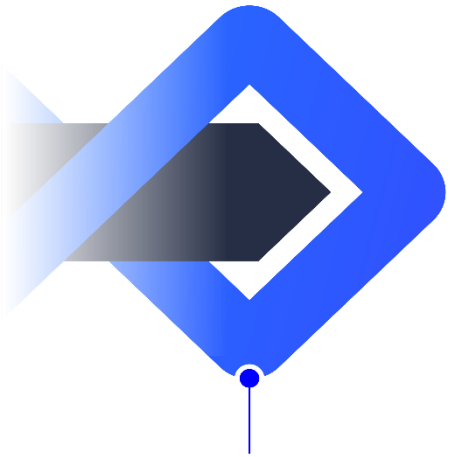
Yet there are other ways of bypassing email security





An Opportunity to Talk About the Challenge

How do you know the cybercriminal's goal?



Complete mission

Using collected intel,
execute mission goal

A Layered Approach Can Do so Much More!

Protect

Advanced email threat protection
Azure AD multi-factor authentication
Advanced email encryption

Detect

Security audit (detect and alert)
AETP 24/7 threat protection

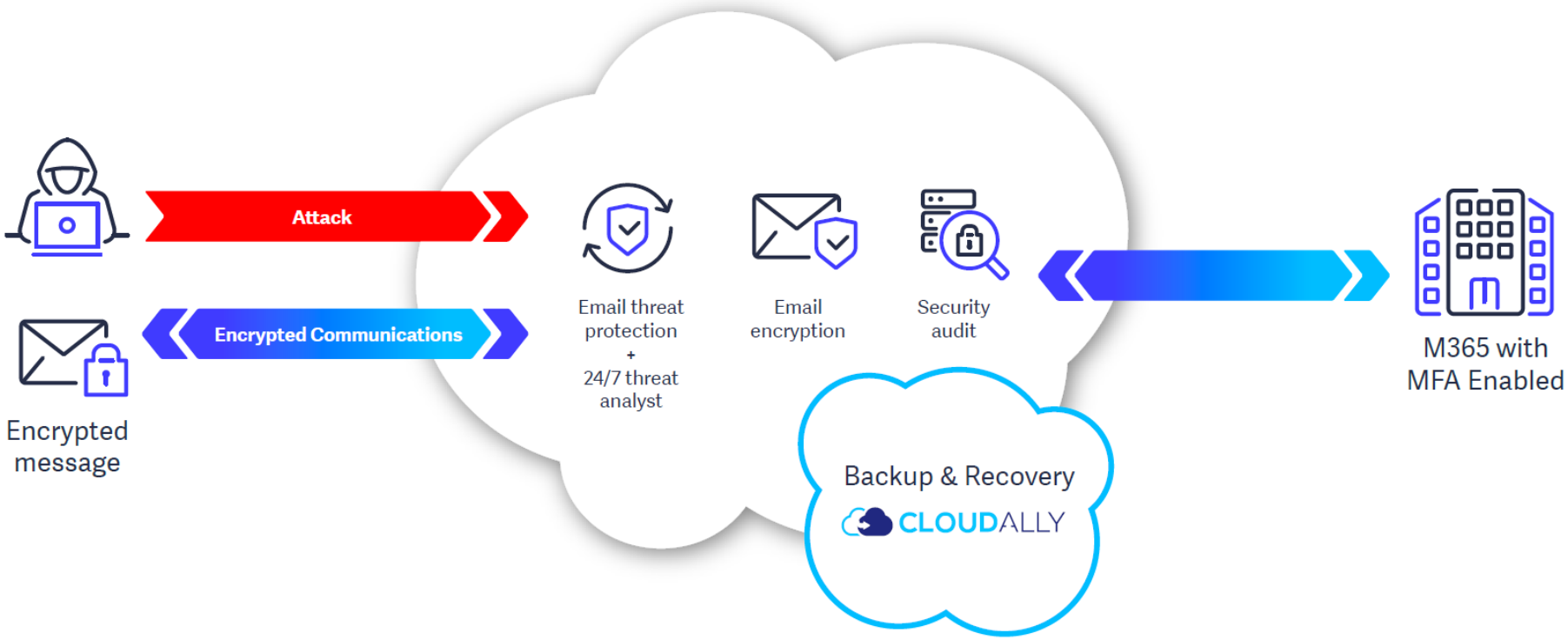
Respond

Security audit (remediate)
AETP (message retraction)
Backup and Recovery
Advanced email encryption (DLP)

zix | appriver

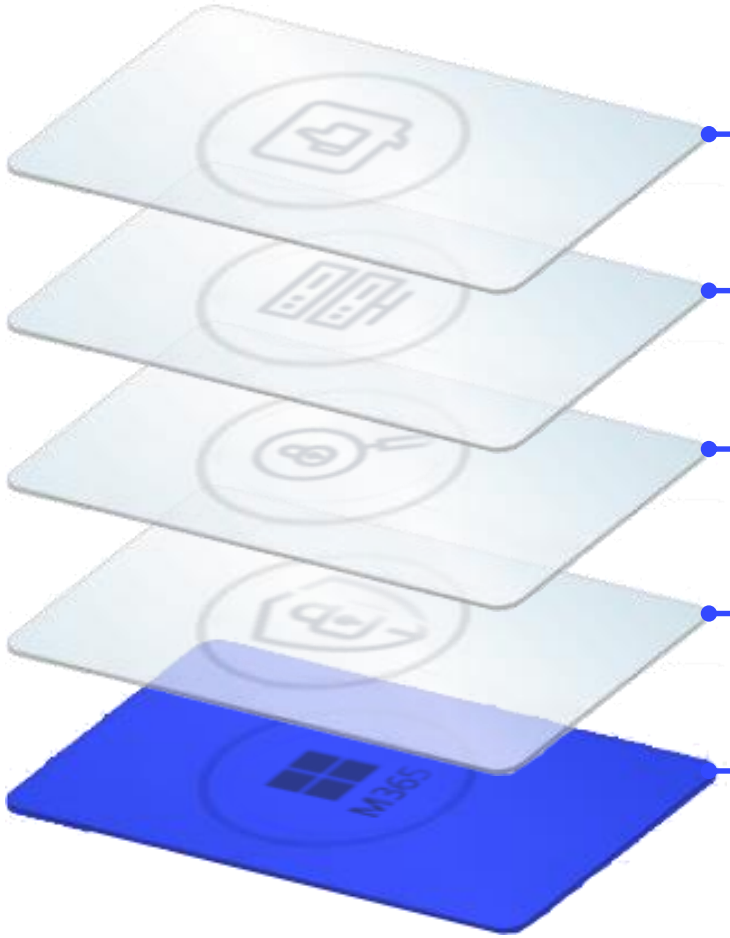
A Layered Approach Can Do so Much More!

Zix simplifies stopping sophisticated cybercriminals



zix | appriver

Zix Layered Security Approach



Phenomenal support for M365
Quick, effective support

Back up for M365
Critical business resilience

M365 Security Audit
Insight and remediation

Email security for M365
Peace of mind security

M365 CSP

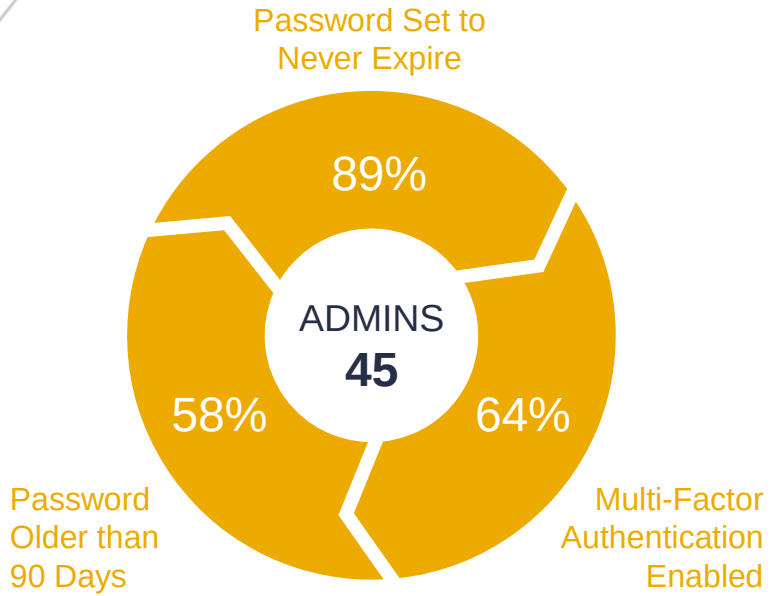
Prevent & Detect

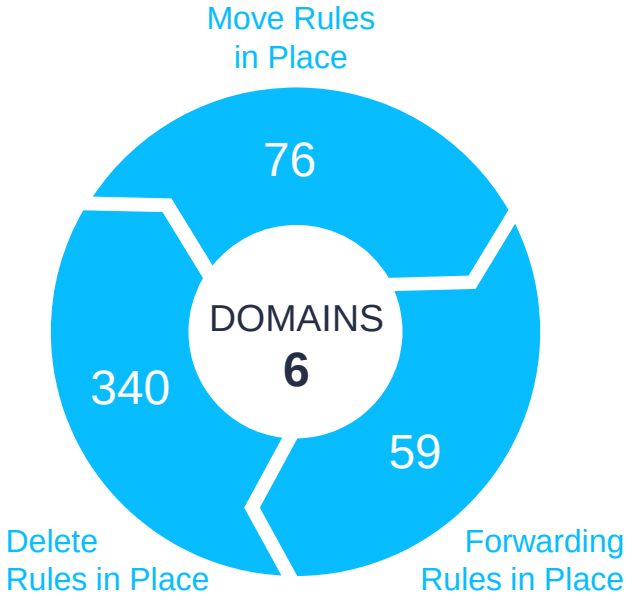
Security Insight You Can Use

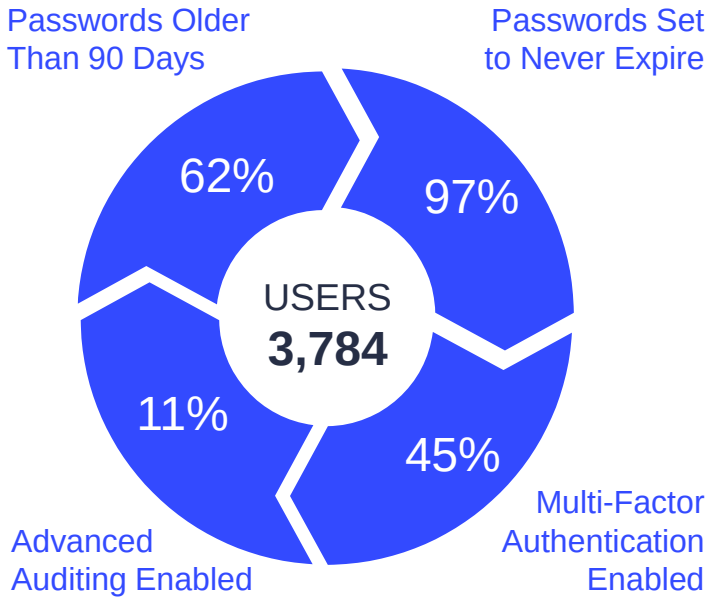
M365 Security Audit

Automated auditing for security insights that make prevention and detection of threats against your productivity suite as simple as one click.

Security Insights







zix | appriver

Microsoft 365 Security Audit Service

- Assesses configurations, summarizes results with clear indicators.
- Identifies gaps and potential compromise.
- Provides key corrective actions the admin can take to secure their tenant and data.

zix | appriver

The Features

Admin Role Report

- Lists all users with admin roles
- Remove admin roles

User Report

- View password policy and MFA status
- Block sign-in

Mailbox Report

- View mailbox access IP and country
- Enable basic and advanced mailbox auditing

Forwarding Report

- Lists all forwarding rules
- Prevent end users from creating forwarding rules
- Disable forwarding rules

InboxRule Report

- Lists all inbox rules
- Disable suspicious rules

Report Scheduling

- Schedule audits for one or more customers
- Create reoccurring audit report jobs

The Benefits

Admin Role Report

- Identifies users with elevated roles
- Guides customer to respect the rule of least privilege

User Report

- Gain insight into unauthorized access
- Quickly remediate compromised accounts

Mailbox Report

- Enables the logging of IP address
- Enables logs for forensic investigation

Forwarding Report

- Help prevent sensitive data leakage
- Ensure employees are not forwarding email to personal accounts

InboxRule Report

- Detect compromised accounts
- Shows how the bad actor was moving through the environment

Report Scheduling

- Time-savings by reducing need to run individually
- Coordinate reports with scheduled customer touch points

Next Steps

Consult with Your Partner

- Scantron has access to our entire suite of security solutions to better protect you from impending threats.

Schedule a Security Audit

- Work with ScanTron to schedule your Microsoft 365 Security Audit today.

Questions?