egress

How to turn a hacker's toolkit against them

AN EGRESS REPORT

What’s inside

Introducing the hacker's toolkit

The cyber threat landscape has rapidly evolved over the past few decades. We've come a long way from the Melissa virus reaping havoc in 1999 through a mass-mail macro, to today's highly targeted and persistent threats. Modern hackers have access to a number of tools (many of which can be accessed legally) which help them make significant financial gains from cybercrime.

These toolkits essentially democratize cybercrime, making it far easier for non-technical cybercriminals to create and launch sophisticated, targeted attacks. Cybercriminals often specialize in a specific role and sell on information that can be used by others in another stage of an attack. These roles can be aligned with the cyber kill chain, with specific tools being used by hackers at each of its stages to achieve their objectives.

There are many readily available tools that can help with all stages of the kill chain, from exploit databases used during reconnaissance, to tools which dump password hashes to enable lateral movement during the later stages of an attack. Understanding these tools and tactics is essential for cyber security practitioners and vendors to enable them to create defenses.

Egress' research focuses on toolkits related to email attacks, as that's the primary delivery mechanism for the vast majority of threats. Our threat intelligence team analyze thousands of phishing emails created by toolkits and investigate ways to reverse engineer these repeatable elements against hackers. Attackers can change the content, graphics, and payloads – but the right technology can detect the telltale signs of a phishing kit in the underlying structure of the email, its context, and delivery mechanism.

Here, we outline some of the tools, tactics, and workflow contained in a hacker's toolkit and explain how to defend against them during the first three stages of the kill chain – **reconnaissance**, **delivery**, and **weaponization**.

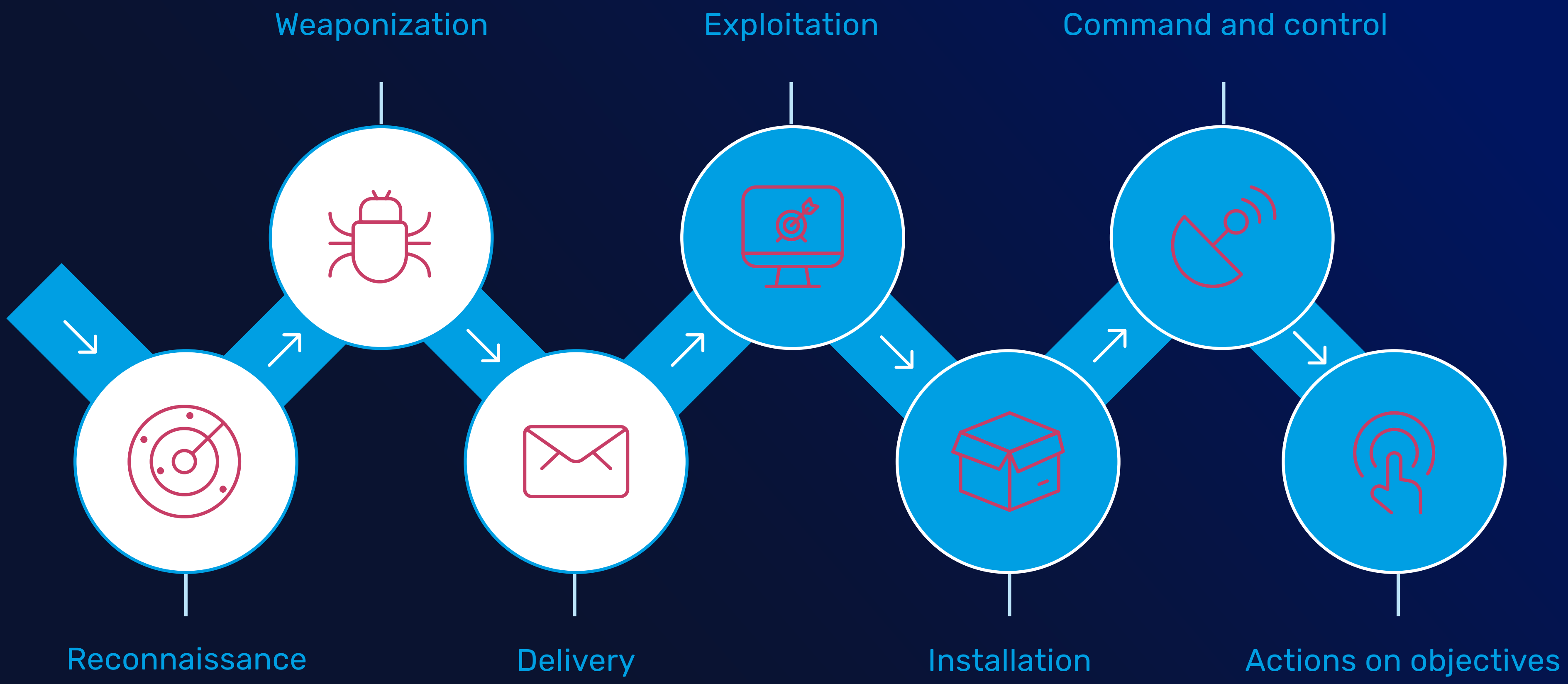


Illustration 1: Steps of the kill chain

How your private information (and security secrets) are gathered

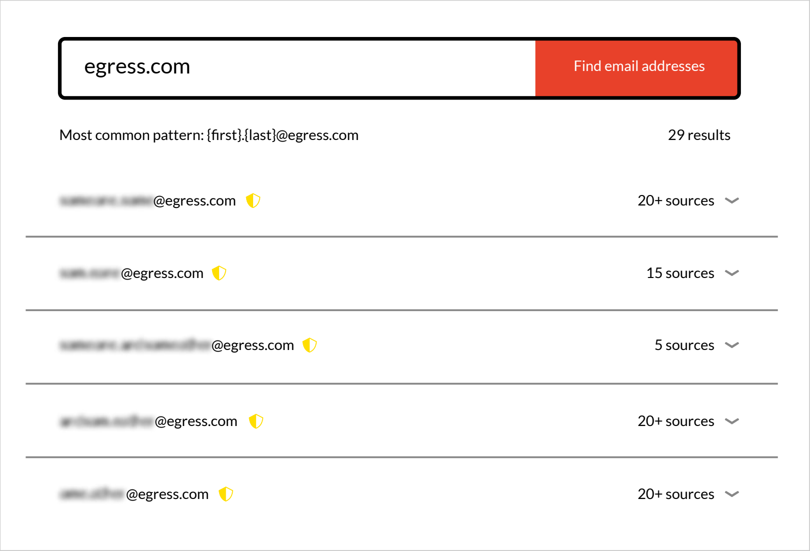
Reconnaissance is the first stage of the kill chain, where a bad actor sets out their objectives, finds a suitable target, and researches the defenses in place. The more information an attacker can gather about a target organization and the individuals within, the better their chances of crafting a successful attack in the next stage (weaponization).

Searching for the right target

A bad actor might choose to Google the top 500 companies by employee count, then narrow down their search from there. Once they've chosen an organization, they can get even more specific and find individual email addresses by using tools typically designed for finding contact details for marketing purposes (figure 1).

Assessing an organization's security posture

Next, the bad actor needs to discover which technologies the target organization is using. The tools to so include databases typically available to marketers. Once the bad actor understands the technologies in use, they can use a public database to discover whether any existing vulnerabilities can be exploited.



egress.com

Most common pattern: {first}.{last}@egress.com

29 results

```
[redacted]@egress.com                20+ sources
[redacted]@egress.com                15 sources
[redacted]@egress.com                5 sources
[redacted]@egress.com                20+ sources
[redacted]@egress.com                20+ sources
```

Figure 1: Example of a marketing tool that can find corporate email addresses

Discovering email security

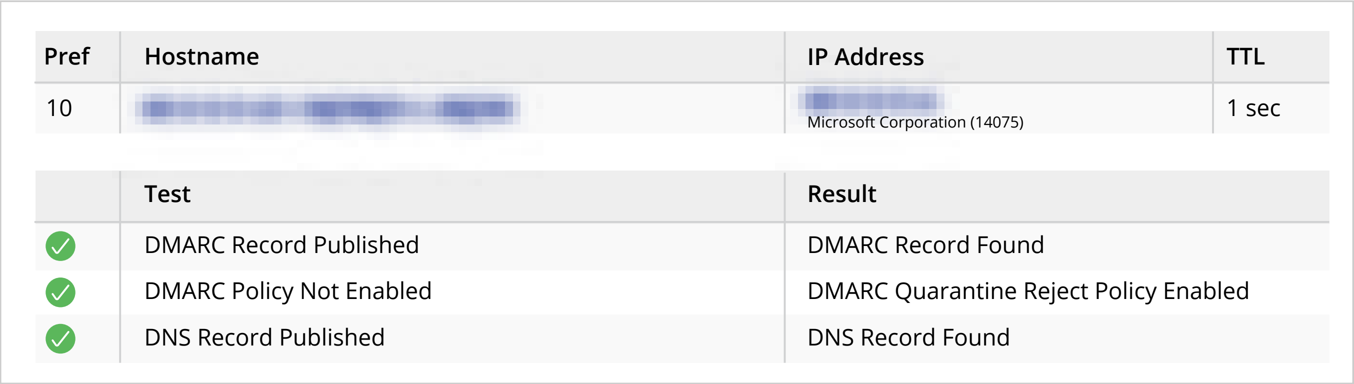
There are various free-to-use tools that a bad actor can use to see what they’re up against in terms of email security. For example, they can perform a DNS MX record lookup on the target’s domain to determine what email security solution they have implemented.

In this case (figure 2), the bad actor has discovered that the target is using Microsoft 365 with no secure email gateway to do any pre-filtering. The hacker now knows their target is reliant on Microsoft 365’s native security features, so if they understand how to evade its security, the email threat will be delivered.

Microsoft 365 is ubiquitous, and the bad actor can easily acquire an account to test their attack. What they cannot assess at this stage is whether the target is using an email security product that inspects emails post-delivery to Microsoft 365.

Assessing which individuals might fall for an attack

The bad actor now sends scouting emails to the intended victims to determine whether they are likely to fall for a phish. These use trackers that show whether the recipient has opened and engaged with the email, and give away their IP address/location. This is all information that can be used later to socially engineer the target individuals – and it can all be achieved via tools used for legitimate marketing reasons.



Pref	Hostname	IP Address	TTL
10	[redacted]	[redacted] Microsoft Corporation (14075)	1 sec

	Test	Result
✓	DMARC Record Published	DMARC Record Found
✓	DMARC Policy Not Enabled	DMARC Quarantine Reject Policy Enabled
✓	DNS Record Published	DNS Record Found

Figure 2: DNS MX record lookup

Further investigating individual targets

The attacker now has a list of people they know might fall for a phishing attack, so they need to understand who might be the most useful person to compromise. They use social media platforms to determine who might be a good target for specific types of attack. For example, they could easily find out who works in a finance role by researching job titles on LinkedIn.

They also gather information about the target individual’s personal life and interests, which will help craft a sophisticated social engineering attack. Finally, they will try to discover whether the target has had personal data exposed from a previous breach. This might include a phone number that can be used in an attack that impersonates a service using text-based multi-factor authentication (MFA).

Defending against **reconnaissance**

We all live our lives on the internet, both professional and personal. It is unlikely that an organization would, or even legally could, force employees to remove information about themselves from social media. However, you can use targeted security awareness training (SAT) to help people understand the impact of their social media activities and be wary of oversharing sensitive information, or accepting connections from suspicious sources.

You can also limit a bad actor from performing some types of attack. For example, senior staff members are often impersonated, so their email addresses can be added to an email security impersonation protection policy. Advising these people to not update their LinkedIn profile until they have been added to the protection policy will help to mitigate these types of attack.

Similarly, trying to keep your technology stack secret is almost impossible. As a protective step, best practice is to ensure that all applications are patched to the latest revisions. You can also perform regular penetration testing and red team exercises to highlight vulnerabilities in technology, processes, and people. This will also allow your organization to understand what information is available to a bad actor, and you can then tailor your security policies with this in mind.

Crafting an attack: How emails are weaponized

The second stage of the kill chain is weaponization, where an attacker determines the payload they want to deliver to the target. The payload might be an attachment containing malware or links to websites that farm credentials or host downloadable malware.

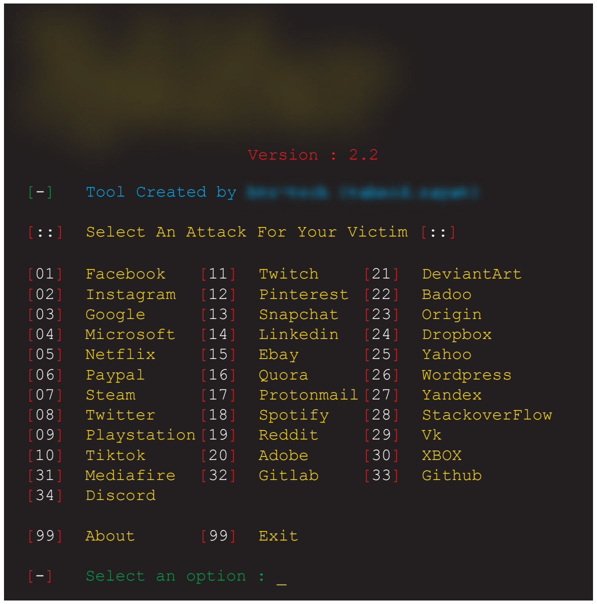
Many email attacks no longer carry a traditional payload, which makes them more difficult to detect. For example, a business email compromise attack uses text-based social engineering to coerce the recipient to transfer money to an account under the control of the attacker. These attacks tend to be referred to as 'payloadless', although one could argue that the text and context of the email itself is the payload.

Creating a spoof website to steal credentials

There are many phishing kits available that spoof common cloud applications and allow hackers to steal their target's credentials. The more expensive ones will include tactics to evade detection by cybersecurity technologies. These include:

- HTML obfuscation techniques using encryption, encoding, and whitespace
- IP address blocklists to identify and block connections from security vendors attempting to scan the webpage for signs of a threat
- User agent blocking (again to identify and block connections from known security crawlers)
- Use of compromised or legitimate sites for hosting

If the bad actor has decided that the target has little security in place and the individual is likely to fall for a phish, they can create spoofed web pages via freely available tools which can be installed onto a compromised server or the hacker's own.

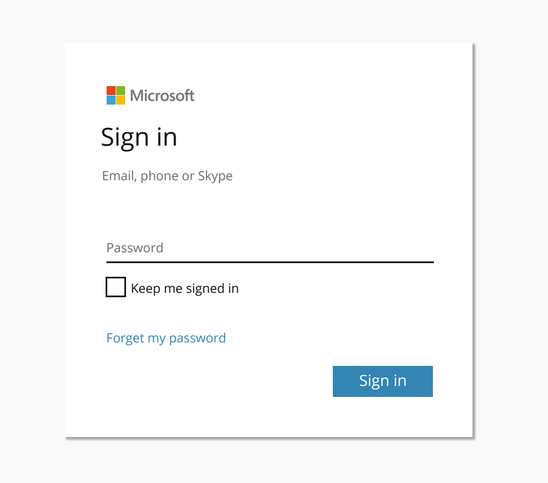


```
[redacted]

                          Version : 2.2

[-]   Tool Created by [redacted]

[::]  Select An Attack For Your Victim [::]

[01]  Facebook    [11]  Twitch     [21]  DeviantArt
[02]  Instagram   [12]  Pinterest  [22]  Badoo
[03]  Google      [13]  Snapchat   [23]  Origin
[04]  Microsoft   [14]  Linkedin   [24]  Dropbox
[05]  Netflix     [15]  Ebay       [25]  Yahoo
[06]  Paypal      [16]  Quora      [26]  Wordpress
[07]  Steam       [17]  Protonmail [27]  Yandex
[08]  Twitter     [18]  Spotify    [28]  StackoverFlow
[09]  Playstation [19]  Reddit     [29]  Vk
[10]  Tiktok      [20]  Adobe      [30]  XBOX
[31]  Mediafire   [32]  Gitlab     [33]  Github
[34]  Discord

[99]  About       [99]  Exit

[-]   Select an option : _
```

Figure 3: A tool used to create spoofed web pages

The bad actor simply selects the website or cloud application they want to spoof. In this example (figure 4) they created a spoof of a Microsoft 365 login page. Of course, once the victim has fallen for the phish and given away their credentials, their web connection needs to be diverted somewhere. In this case, they are taken to a legitimate login page and will likely think they need to input their password and login again because 'it didn't work the first time'.

A more sophisticated user might be able to spot the fake URL of a spoofed webpage. This problem can be overcome by the attacker, albeit at a cost, by hosting the page on Microsoft Azure, so the page is on a Microsoft domain and presents a valid SSL certificate.



Microsoft

Sign in

Email, phone or Skype

Password

□ Keep me signed in

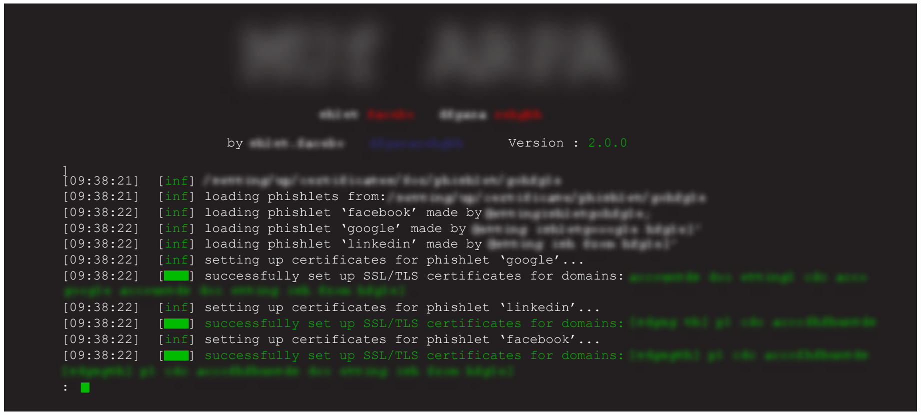
Forget my password

Sign in

Figure 4: Spoofed Microsoft 365 login page

Stealing multi-factor authentication (MFA) tokens

To render credential theft pointless, many organizations use MFA, but there are tools to steal MFA tokens too. Again, these tools are often freely available (figure 5).



```
[redacted]

                    [redacted]

          by [redacted]            Version : 2.0.0

]
[09:38:21]  [inf] [redacted]
[09:38:21]  [inf] loading phishlets from: [redacted]
[09:38:22]  [inf] loading phishlet 'facebook' made by [redacted]
[09:38:22]  [inf] loading phishlet 'google' made by [redacted]
[09:38:22]  [inf] loading phishlet 'linkedin' made by [redacted]
[09:38:22]  [inf] setting up certificates for phishlet 'google'...
[09:38:22]  [███] successfully set up SSL/TLS certificates for domains: [redacted]

[09:38:22]  [inf] setting up certificates for phishlet 'linkedin'...
[09:38:22]  [███] successfully set up SSL/TLS certificates for domains: [redacted]
[09:38:22]  [inf] setting up certificates for phishlet 'facebook'...
[09:38:22]  [███] successfully set up SSL/TLS certificates for domains: [redacted]

: █
```

Figure 5: A tool used to steal MFA tokens

A link payload is generated that will take the target to a page that's a perfect spoof of the cloud application or website. Since this requires a domain to be registered, the bad actor will likely register one that is similar to that of the cloud application or website being spoofed. This will have a higher chance of not being spotted by the target and the attack is more likely to be successful.

The target inputs their credentials, but this time they are also prompted for their MFA token, which can be used to immediately log in to the real site.

Defending against **weaponization techniques**

By understanding the types of payloads that are being used and ensuring your security vendors do too, you can deploy the appropriate defense-in-depth security stack to cover all known eventualities. For example, all email and web security solutions will protect against volumetric, known, and some unknown threat types, as will endpoint security.

To protect against more advanced web-based threats, ensure your email and web security follow links to their final destination and examine the page contents, looking for signs that it might have been created by a phishing kit. Microsoft Defender ATP Safe Links can help with this. Then augment this with intelligent link inspection technologies that learn about the composition of bad links and those that might have been created by a phishing kit, such as Egress Defend.

To protect against zero-day and advanced malware, sandboxing is essential to explode executable files and monitor for suspicious behaviors – you can use Microsoft 365 Defender ATP Safe Attachments for this. If we assume text that attempts to socially engineer the target is a payload, then you need to deploy intelligent technologies that use linguistic analysis to determine whether the subject and body copy might contain signs of a phish.

These advanced technologies typically combine with others associated with the delivery stage to inspect the email holistically and will often detect email threats that contain a malware attachment that has evaded detection by sandboxes.

Hackers’ favorite delivery tactics for evading email security

Stolen credentials offer attackers an easy route into email accounts – some hackers focus their efforts solely on stealing credentials that they then sell on to others. One reason Microsoft credentials are so highly sought after by bad actors is that they can be used to progress an attack using a compromised (but legitimate) account. These will have a higher likelihood of evading detection by email security – especially solutions only inspecting malicious payloads.

Legitimate email sending tools

Emails sent by attackers from legitimate B2B applications such as CRM and marketing platforms will add a layer of credibility to a phish and help it evade detection. Several of these are free to use and easily accessible.

Burner email addresses

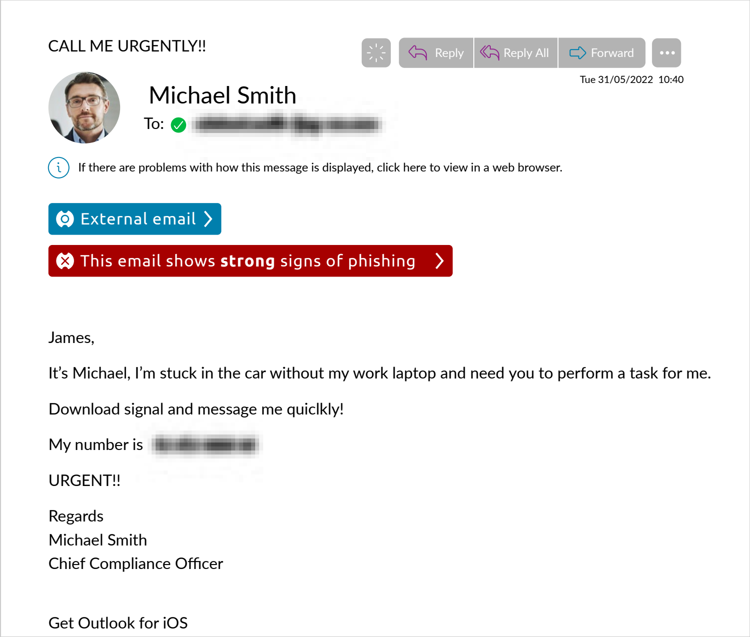
Burner addresses are email accounts that can be easily setup to ensure the bad actor cannot be identified. Services like 10-minute mail provide random addresses that are valid for 10 minutes. Alternatively, webmail services such as Gmail can be used. However, these addresses are often treated as suspicious by email security.

Impersonate trusted individuals

If the hacker can't use a real compromised account, the next best tactic to increase the likelihood of success is to impersonate a trusted colleague, business partner, or customer. No tools are required here, but a combination of Microsoft Azure AD and Outlook provides a significant benefit for the bad actor.

Outlook locates the impersonated sender's details in the 'from' field, searches and finds them in Azure AD, and assigns their contact details to the email. If the recipient hovers over or clicks on the image of the impersonated sender's icon or name, they will see the valid details from Azure AD, which lends authenticity to the email.

In Figures 6 and 7, we show how this tactic works, using email copy from a phishing email that impersonated an Egress senior executive, including displaying their AD record, and was sent to a more junior team member. We've changed the names to protect the identities of the people involved.



CALL ME URGENTLY!!

Michael Smith

To: [redacted]

Tue 31/05/2022 10:40

If there are problems with how this message is displayed, click here to view in a web browser.

External email

This email shows **strong** signs of phishing

James,

It's Michael, I'm stuck in the car without my work laptop and need you to perform a task for me.

Download signal and message me quiclkly!

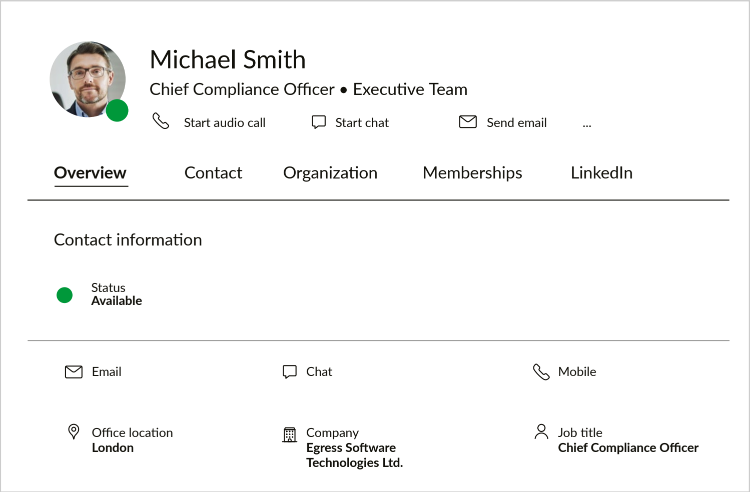
My number is [redacted]

URGENT!!

Regards
Michael Smith
Chief Compliance Officer

Get Outlook for iOS

Figure 6: Example of an attempted impersonation of an Egress senior executive, with anti-phishing warning banners added by Egress Defend (names have been changed to protect the identities of those involved)



Michael Smith

Chief Compliance Officer • Executive Team

Contact information

Status
Available

Email

Chat

Mobile

Office location
London

Company
Egress Software Technologies Ltd.

Job title
Chief Compliance Officer

Figure 7: Example of an Azure AD record, which can be displayed when Outlook locates an impersonated sender's details in the 'from' field

Defending at **the delivery stage**

Security technologies to prevent attacks penetrating the business are pervasive. However, organizations recognize that none are 100% effective, so they adopt defense-in-depth and also deploy response and remediation tools.

The 2022 Verizon Data Breach Investigations Report revealed that 82% of data breaches involved a human element. SAT is essential to help users understand, for example, what a phishing email that has been delivered to their inbox looks like. However, it needs consistent, regular reinforcement to prevent the human error that results in breaches. You can help reinforce SAT by using an email security solution that adds dynamic information to an email that highlights signs of suspicion. Simple adding a blanket warning to every email that states it is from an ‘external source’ leads to notification fatigue and adds little valuable information for the user to help them understand the nature of the risk.

Most traditional email security solutions provide defenses directly related to delivery that are combined with payload inspection to determine whether an email is suspicious. These include authentication technologies, such as DMARC, DKIM and SPF, header analysis, and sender reputation checks.

In the past few years, the move to cloud email platforms that provide mail flow rules and APIs for post-delivery claw back of emails for inspection has resulted in a new type of email security solution: integrated cloud email security (ICES, coined by Gartner). Most do not attempt to replicate the security already in use, but to augment it with innovative intelligent detection techniques. These include machine learning, linguistic analysis, and social graph technologies to detect highly targeted, sophisticated, and payloadless attacks.

Social graph technology, in particular, is directly related to delivery. It creates a baseline of trust by monitoring sender/recipient communications and treats anomalies as suspicious. Of course, given the problem of compromised accounts, none of the technologies related to delivery should be used in isolation or over-relied on.

›› Key takeaways on turning toolkits against the hackers

When considering technologies to defend against attacks reaching their targets, organizations should consider security vendors with professional threat research teams whose sole purpose is to understand bad actors' tactics, techniques, and procedures. By thinking like a hacker and understanding the tools they use, effective defenses can then be crafted.

For example, Egress threat researchers have spent considerable time analyzing emails that are created by phishing kits. To evade detection, when kits generate emails, they automatically change the content, copy language, graphics, and payloads. However, Egress Defend instead looks for the underlying structure of the email that cannot be changed.

By focusing intelligent detection technologies on the delivery mechanism and understanding the context of the payload rather than the payload itself, which will already have been inspected by an organization's traditional SEG or Microsoft 365, Egress Defend completes a defense-in-depth approach to email security.

About Egress

Our mission is to eliminate the most complex cybersecurity challenge every organization faces: insider risk. We understand that people get hacked, make mistakes, and break the rules. To prevent these human-activated breaches, we have built the only Human Layer Security platform that defends against inbound and outbound threats. Using patented contextual machine learning we detect and prevent abnormal human behavior such as misdirected emails, data exfiltration and targeted spear-phishing attacks. Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York and Boston.

www.egress.com | in Egress Software

egress