# Russia-Ukraine Proofpoint Security Insight & Recommendations

Proofpoint

# What’s in this deck

- Russian actor activity & how to find Russian actor activity in your account
- Taking further, more aggressive, proactive Security measures
- Proofpoint’s Posture

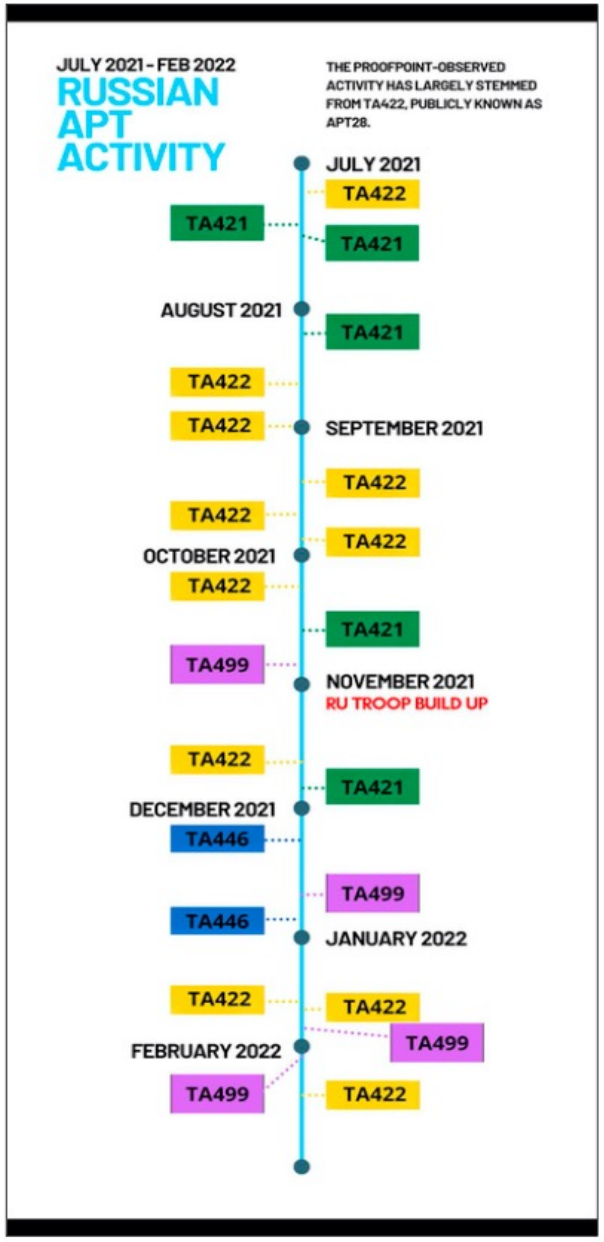
# Geo-Political Tensions

## What You Need to Know

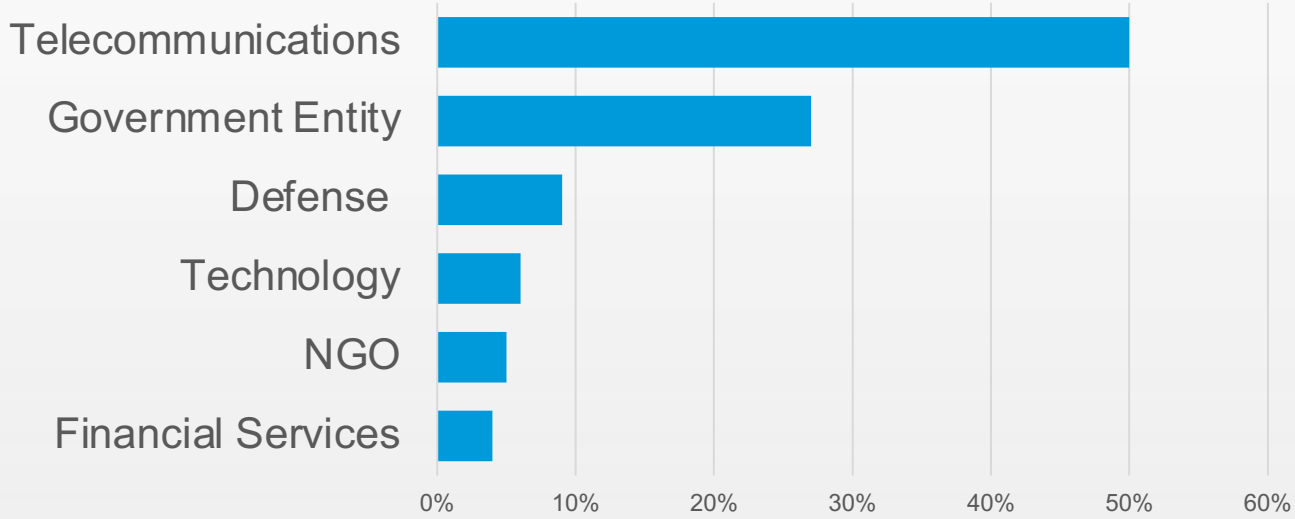
- On February 24, Russia authorized a “special military operation” against Ukraine and shortly thereafter military action commenced inside of Ukraine borders.
- Various sanctions against Russia are being imposed by the West, and consequently, increased cyber operations against Western targets are very likely.
- Leading up to this operation there have been reports of distributed denial-of-service (DDoS) campaigns targeting financial institutions and government agencies. Additionally, there have been reports of wiper malware infecting systems in Ukraine.
- Proofpoint has not observed mass or out of the ordinary email delivery campaigns from Russian State Actors, however we are monitoring the situation very closely and are adjusting defenses accordingly.
- Proofpoint will notify customers when we observe any state-aligned activity targeting their users.

Update: Feb 24th:

- Proofpoint is tracking public reports of wiper malware, dubbed HermeticWiper, being used against Ukrainian and Latvian machines, as well as early reports of a new ransomware written in Go spreading through Ukraine. Sandbox and Emerging Threats signature content has been developed to detect these threats.




## Recent Russian APT Targeted Sectors



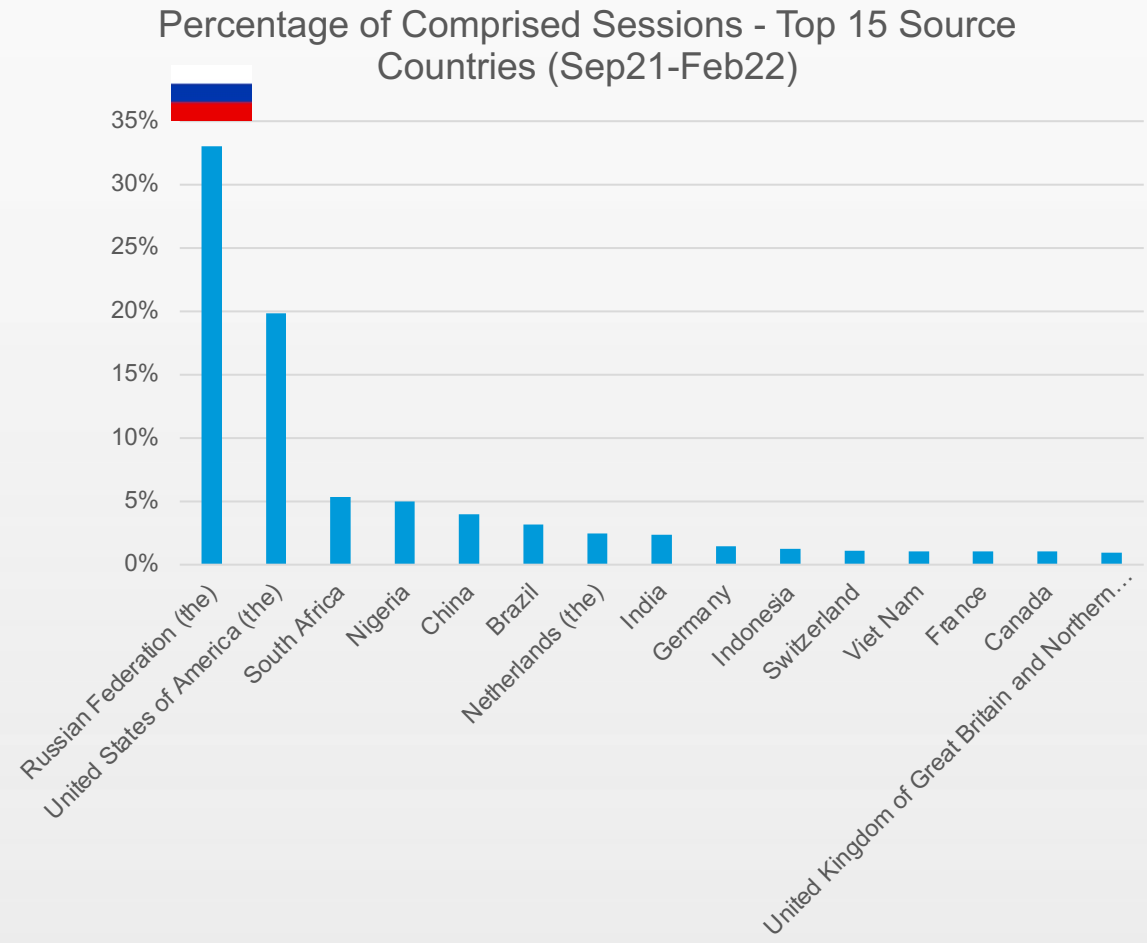

proofpoint.

# Account Takeover is an attack vector by Russian Actors

| | Brute Force / Credentials Variance Attacks | Email Based Attacks* |
|---|---|---|
| Orgs Targeted | 96% | 65% |
| Orgs Compromised | 26% | 42% |

*Credential phish, malware and more

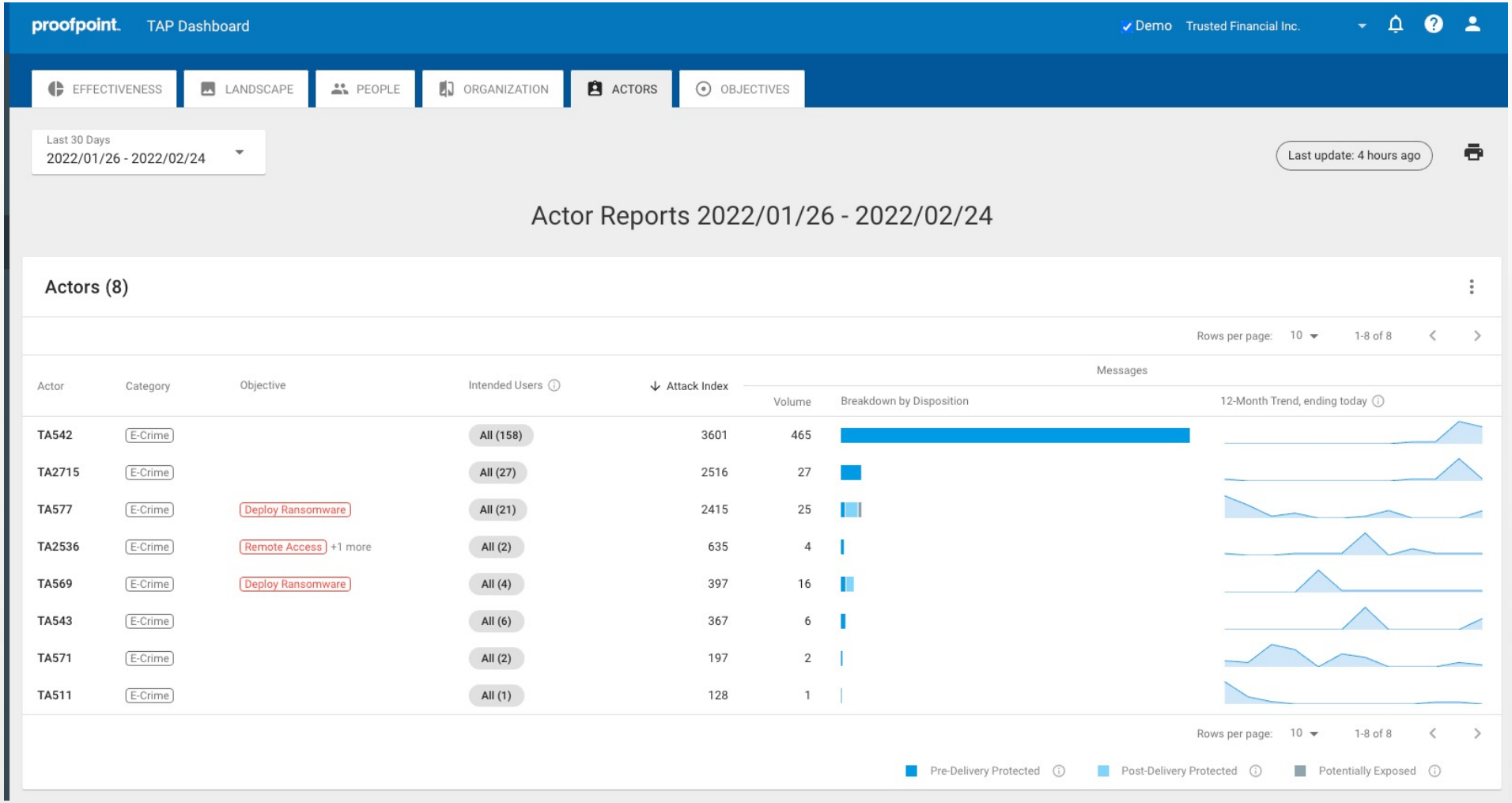
Source: Proofpoint, H1, 2021




Sources include proxy services

proofpoint.

# TAP DASH Actor view will tell you who is targeting you



# Look for these actors in your data (part 1)

## Russia | TA421 | APT29, Dukes, Cozy Bear

**Key Points:** TA421 is a state-sponsored threat actor originating from Russia. This actor focuses on intelligence gathering, broadly targeting US government entities, universities, think tanks, and ministries of defense and foreign affairs worldwide. TA421 has been known to leverage Adobe Reader vulnerabilities, documents with malicious macros, Zip attachments, malicious links, and compromised websites in its campaigns. The threat actor most recently has utilized the shared malware Cobalt Strike in its 2021 campaigns.

## Russia | TA422 | APT28, Sofacy, Sednit, Strontium, Pawn Storm

**Key Points:** TA422 is a Russia state-sponsored actor. In 2018 the US Department of Justice confirmed that the threat actor is Russian military intelligence. TA422 has a range of targets from ministries of defense and foreign affairs worldwide to journalists, think tanks, US political entities, and aerospace organizations. The threat actor typically sends multiple emails to targets including those with malicious attachments and links intended to harvest credentials. TA422 also uses rented and multilayered infrastructure, leveraging virtual private servers paid with bitcoin.

## Russia | TA499 | Vovan and Lexus

**Key Points:** TA499 is believed to be an impersonation-based, patriotically motivated misinformation pair of actors aligned with the Russian state. This threat actor leverages benign email campaigns to solicit information from high-profile individuals and convince targets to participate in recorded phone calls or video chats. The targets are typically those who have spoken out about the Russian regime, in favor of sanctions against Russia, and against the arrest of Russian opposition leader Alexei Navalny.

# Look for these actors in your data (part 2)

## CIS | TA445 | Ghostwriter

**Key Points:** TA445 is likely a Belarusian state-sponsored threat actor; however, the group is suspected to hold ties to Russia through either training or technical contributions provided by
Russian threat actors. TA445 focuses its espionage efforts against the defense and media verticals, among others. This threat actor appears interested in not only compromising its targets but using them to disseminate falsified information. Disinformation spread by TA445 is particularly focused on Poland's military activities, anti-United States sentiments, and criticism of the North Atlantic Treaty Organization (NATO).

## CIS | TA446 | Callisto Group

**Key Points:** TA446 activity historically has aligned with Russian interests, but the degree to which the group works directly for the Russian government is unknown. The threat actor targets former government employees that have moved into high level positions of interest at private corporations. TA446 typically starts their campaigns with benign emails then sends phishing emails with malicious links intended to harvest credentials. TA446 frequently masquerades as individuals known to or affiliated with the target or the target's profession.

# Options in Proofpoint Products to Defend Against State-Level Attacks

# Proofpoint Levels of protection progression

| General Best Practices | Level 1: Tighter Enforcement & exec protection | Level 2: Harden Defenses with some experience compromise | Level 3: Limit communication modes |
|---|---|---|---|
| • Enforce best practices with Proofpoint product<br>• Have a communications availability plan<br>• Impact:<br>  ○ Business as usual state<br>  ○ Little to no additional impact | • Additional Protection for VIP/C-Suite<br>• Stricter enforcement of best practices<br>• Impact:<br>  ○ Higher chance of quarantining good email<br>  ○ Possible delay of some messages<br>  ○ Some user experience impact | • Increase blocked mail with tighter anti-spoof, spam, and imposter rules<br>• Stricter use of TAP (eg no Password protected files)<br>• Impact:<br>  ○ May lead to higher False Positive rate<br>  ○ Possible delay of messages due to lengthening Sandbox timeouts | • Block all attachments<br>• Remove all safelisting<br>• Defang all URL's<br>• Impact:<br>  ○ More messages quarantined, delaying delivery<br>  ○ Significant impact to business as usual<br>  ○ End user experience will be disrupted |

proofpoint.

# General Best Practices

## Recommendations

- Implement all recommendations in the Proofpoint Health Check report for your Proofpoint Threat Platform
- Ensure that RDP and other internet-exposed network resources are carefully secured and critical and/or legacy systems are appropriately segmented.
- Immediately remediate delivered threats, particularly those associated with known initial access brokers, many of whom likely operate in or near the region and have established footprints across Western organizations.
- Alert on Cobalt Strike traffic and potential signs of data exfiltration or C2 communications via network signatures such as those provided by Proofpoint Emerging Threats
- Visit Proofpoint Communities for updates & consider enlisting in our Premium Threat Services Program to understand specific threats in your environment

# Level 1 Recommendations

| Product | Recommendation | Detail |
|---|---|---|
| Email Protection (PPS Console) | PPS System configuration changes | Stop accepting mail from unresolvable domains<br>• on-premise only<br>• can impact internal mail if DNS is not properly configured |
| | Stricter administrator login requirements | • Restrict admin console logins based on IP address/range of the customer's network<br>• Integrate admin login with customer's SAML single sign-on and enable multi-factor authentication |
| | Targeted Attack Protection – Attachment Defense | Increase attachment scanning timeout to 30 minutes |
| | Improve SPAM effectiveness | • Configure ***Circle of Trust*** for executives & VAPs<br>• Set ***Spam Definite*** threshold to 98 |
| | Email Warning Tags | Enable all email warning tags (*This message came from an external source, please use caution, etc*) for all users |
| | Create Email Firewall rule(s) based on geolocation information | Quarantine/Discard messages based on country codes & domains of concern (*.ru) |
| | DMARC – Enable full enforcement of all DMARC records | Enable ***norecordfailspf*** rule and set disposition to Reject |

proofpoint.

# Level 1 Recommendations (continued)

| Product | Recommendation | Detail |
|---|---|---|
| Isolation | Add all users to Isolation with a “low” security policy | Include at least a limited number of redirect categories with Proofpoint-recommended exceptions |
| | Add high value targets/VAPs/VIPs to a “medium” security policy | Redirect all categories of URL to Proofpoint Isolation, including Proofpoint-recommended exceptions |
| | Require all personal email to go through Email Isolation | Redirect all personal webmail services to use Email Isolation for all users |
| CASB | CASB rule to detect logins from countries/areas of concern | Monitor for suspicious logins to any cloud applications and alert for later auditing |
| ITM | Create alerts based on our knowledge of email and web threats. | If an email has a known subject line or a URL for a known malicious domain, we could import these values into ITM and configure alerts to fire immediately to the SOC team. |

# Level 2 Recommendations

| Product | Recommendation | Detail |
|---|---|---|
| Email Protection (PPS Console) | Stricter anti-spoof protections | Configure ***pp_antispoof*** firewall rule disposition to Quarantine & Discard to help protect against email addresses in comment section of *From:* header |
| | AntiVirus – Block all password-protected attachments | Quarantine and discard for password protected attachment. Recommended that this is NOT included in digest or end user web to be visible by end users. |
| | Encrypted containers (PGP, S/MIME) | Quarantine and discard messages identified as PGP or S/MIME Encrypted. |
| | Email Firewall – Create an email firewall to prevent Internationalized Domain Name Spoofing | In the example, when this email reach the inbox, it would look like it came from proofpoint.com.<br><br>/usr/bin/swaks --to 'jdoe@proofpoint.com' --from 'jdoe@diagnostic.email' --server 'mxa-1234567.gslb.pphosted.com' --h-From: '"John Doe" jdoe@xx--proofpoint-om26a.com' --h-Subject 'Test Message [Internationalism Domain Spoofing] [RunId: 27da47bb]' --suppress-data --silent 2 --add-header 'X-Mail-Test: Proofpoint' --body 'Hello, This is a test message. |
| | Adjust Impostor threshold | Set the Impostor score to 70 |
| | Configure additional blocklist | Add SORBS as a DNS blocklist source |
| TAP (in PPS Console) | Targeted Attack Protection - Attachment Defense | Increase attachment scanning timeout to 60 minutes |
| | Targeted Attack Protection - URL Defense | Enable ‘Aggressive’ rewriting of URLs |

proofpoint.

# Level 2 Recommendations (continued)

| Product | Recommendation | Detail |
|---|---|---|
| Isolation | Add all users to Isolation with a “medium” security policy | • Add high value targets/VAPs/VIPs to a “high” security policy<br>• Block personal webmail for high value targets<br>• Block clicks for all URLs going to Russia & other countries of concern<br>• Block clicks to file sharing services not used/authorized by the organization |
| CASB | Create Email Firewall rule(s) based on geolocation information | Monitor for suspicious logins to any cloud app and set to *Terminate Session* for successful logins based on country of origin. |

proofpoint.

# Level 3 (High) Recommendations

**(all items from the Medium list, plus the following)**

| Product | Recommendation | Detail |
|---|---|---|
| Email Protection (PPS Console) | Block all non html/text/images incoming attachments | Configure ***exestrip*** firewall rule to remove all attachments from incoming messages |
| | Enforce rules based on geolocation | Quarantine & Discard all incoming messages from countries where the organization does not normally do business. |
| | Spam policies | Disable *Safe* rule (will disable safelisting for both the global safelist, and the end user safelists) |
| | TAP Attachment Defense | Configure *Timeout* rule disposition to Quarantine & Discard |
| | TAP URL Defense | "Defang" all URLs using special filter.cfg entry: *com.proofpoint.filter.module.urldefense.policy.<policyid>.defangurls=t* |
| Isolation | Enable stricter Isolation policies & options | Add all users to Isolation with a “high” security policy + disable "Exit Isolation" option |
| | | Block clicks for all URLs going to Russia & other countries of concern |
| CASB | CASB rule to detect activity from Russia (& other suspected countries) | Monitor IP login failures to any cloud app and set to Terminate Session **and** *Suspend Account* for successful logins based on country of origin. |

proofpoint.

# Mail Clients/Store recommendations

| Product | Recommendation | Detail | Level |
|---|---|---|---|
| Email Client (Outlook, etc....) | Prefer the "text" version of messages | Configure client to prefer displaying the "text/plain" version of an email instead of the "text/html" version. | 3 |
| | Disable use of Mobile Devices | Mail clients on Mobile devices usually show less security related informations. As a last resort solution disabling email access from these devices might be an option. | 3 |
| | Isolate all Email | Require all Web clients to be Isolated for Email access both personal and corporate (level 1 for personal, leve 2 for corporate) | 2 |
| | Block access to personal Webmail | Block consumer Webmail access from corporate network/devices. | 3 |
| | Wait 20 minutes before reading an external email | By waiting, you give time to the security gateways, and possibly the Proofpoint TRAP product to leverage new threats and remove offending messages. | 2 |
| Office365 / Exchange Online | Prevent direct delivery | Block unauthorized deliveries directly to Exchange online by using connector configuration ("*" as scope, restricted to Proofpoint IPs + your own known relays). | 1 |
| | Enable MFA for all accounts | Ensure you are using Multi-Factor authentication for access to Office 365 | 1 |

# What Proofpoint is doing

# Dynamic Defenses for a Heightened Threat Environment

## Proofpoint is taking actions to elevate our security posture in light of the situation with Ukraine

1. Temporarily elevating the protections provided by our People Centric Security situational controls, for example, enabling more time for attachments to be evaluated by TAP Attachment Defense
2. Ensuring that network protections are operational and ready, including distributed denial of service (DDoS) detection and mitigation controls.
3. Conducting threat hunting exercises, leveraging Proofpoint Cloud App Security Broker, to focus on activity originating from countries of concern
4. Leveraging Crowdstrike threat hunting services to check for indicators of compromise, per plans that were already in place
5. Enlisting the global employee community to be aware of the heightened risk, reminding them to report possible security issues to Global Information Security by using the Report Suspicious button in Outlook
6. Monitoring for the latest intelligence on the threat, leveraging Proofpoint Premium Threat Intelligence Service, as well as guidance from the US Cybersecurity & Infrastructure Security Agency.
7. Maintaining heightened awareness and vigilance on the part of our incident responders, and ensuring the team is at full strength (and enlisting backfills from other teams if necessary).
8. We do not have offices or operations in Ukraine or Russia, so the physical invasion should not impact Proofpoint's ability to deliver our services to our customer base.