Zero Trust Outside The Wire: Combatting Cyber Influence And Espionage Threats

Computational Propaganda, Fake News, And Viral Videos Represent A New Type Of Business Attack With Devastating Consequences

by Chase Cunningham, Nick Hayes, and Jeff Pollard

September 25, 2018

Why Read This Report

Direct cyberattacks that take a bank offline or steal millions of customer records are alarming, but there's an even larger, more dangerous specter of attacks security leaders are unprepared to combat: From AI-powered cyber influence campaigns to the viral spread of highly convincing fake videos, adversaries launch, control, and orchestrate attacks from outside of your secured operations — as the military calls it, "outside the wire." Security leaders must help the business protect its most valuable asset — its brand — by extending Zero Trust concepts "outside the wire."

Key Takeaways

Exploiting Sentiment And Damaging Reputation Is As Harmful As Malware

Sending malicious payloads and packets is no longer the standard in threat operations. In today's world of massive social media presence and influence, malicious actors or threat groups can simply aim a Twitter campaign at their chosen enemy and bring that entity to its knees, 140 characters at a time.

Global Enterprises Are The Next Targets, After Politicians And Nation-States

Manipulating emotion and reputation isn't new, as the 2016 US election illustrates. What happens when bad actors attack your enterprise the same way they attack politicians? Using open source tools, bot farms, and troll factories to target your company and sway public perception, attackers could inflame sentiment and rally the masses against you. Your brand isn't immune to this type of threat.

Zero Trust Applies Outside The Wire

Your business must understand that successful attacks occur outside of the infrastructure your security team traditionally safeguards. Just as you do for networks, identity, and infrastructure, you must apply the concept of Zero Trust outside the wire.

Zero Trust Outside The Wire: Combatting Cyber Influence And Espionage Threats

Computational Propaganda, Fake News, And Viral Videos Represent A New Type Of Business Attack With Devastating Consequences

by Chase Cunningham, Nick Hayes, and Jeff Pollard
with Stephanie Balaouras, Claire O'Malley, Madeline Cyr, and Peggy Dostie

September 25, 2018

Table Of Contents

Related Research Documents

Assess Your Exposure To Geopolitical Cyber Risk

The Forrester New Wave™: Digital Risk Protection, Q3 2018

Using AI For Evil

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Companies Face Unprecedented Attacks On Brand And Reputation

Computational propaganda, fake news, and viral videos represent a new type of attack for companies where virtue signaling is the means and ends of the attack. They damage customer engagement and loyalty and seed widespread distrust capable of crippling the credibility of government and corporate institutions alike. Forrester defines computational propaganda as:

> *Concerted activity with financial, geopolitical, or other explicit motives to sow discord and distribute biased or misleading information at massive scale through the use of powerful computing resources, specialized AI and machine learning, and access to distributed online forums and social networks (and the resulting psychographic data).*

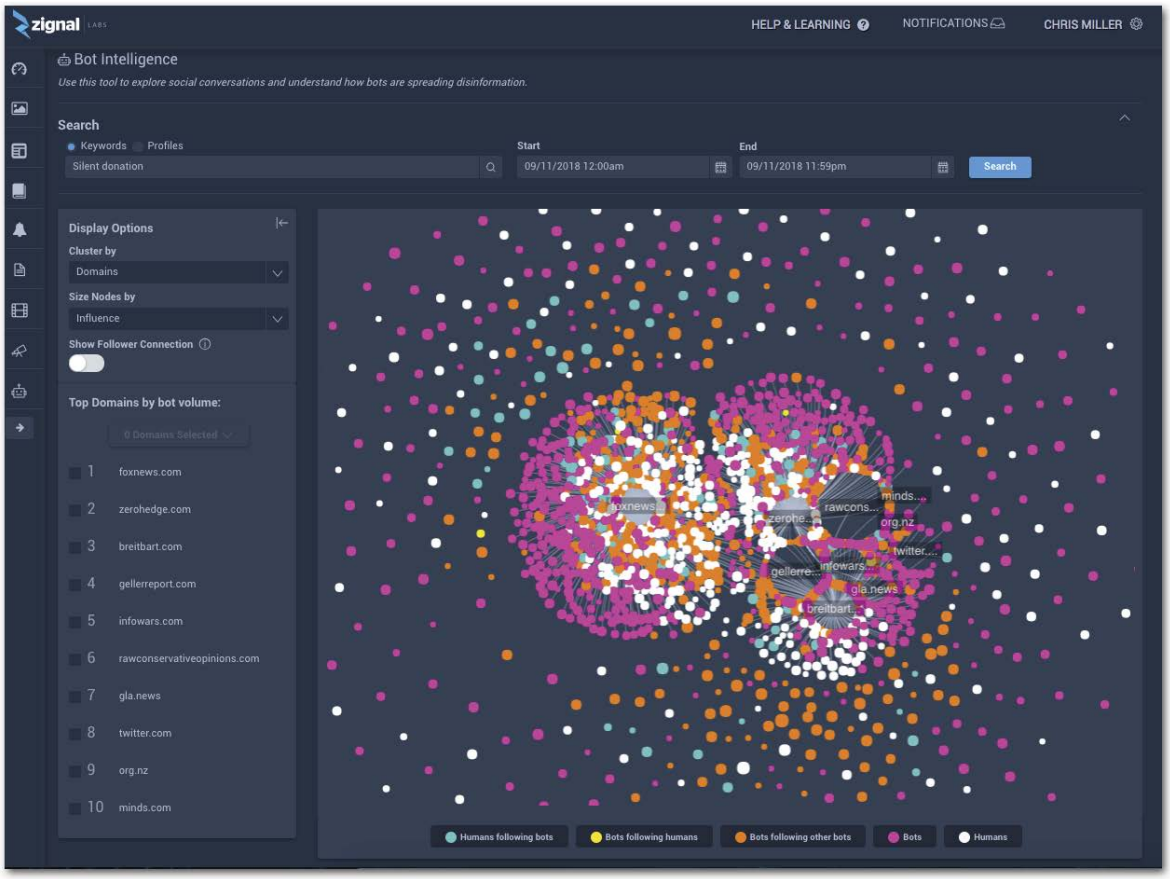
When well executed, these attacks are devastating, targeting firms' valuable digital assets and brand.[1] All it takes is a small group of nimble threat actors, acting independently or at the behest of a competitor, hacktivist group, or nation-state, to execute influence campaigns. These asymmetric attacks are rising threats for organizations, ones which security and risk leaders must address and counter, because:

- **Cyber influence campaigns reach audiences at unprecedented speed and scale.** In World War II, spreading propaganda required artists, printing presses, and airplanes to design and airdrop leaflets aimed at eroding the morale of enemy soldiers. Today, these physical limitations are all but irrelevant. The prevalence of social media and constantly connected devices means campaigns reach audiences instantaneously. And fake news goes viral even faster; in fact, fake news is 70% more likely to be retweeted than true stories.[2] A mechanism once driving customer engagement has turned into a digital risk for firms of any size and location.[3] A bot-led influence campaign targeted Microsoft and amplified negative press about the tech provider's work with US Immigration and Customs Enforcement (ICE); the story was real, but bots generated 52% of the social conversations, adding fuel to already contentious discussions on immigration.[4]
- **Botnets turn mishaps into full-blown crises.** Botnets are coordinated groups of inauthentic accounts built to reach, influence, and disinform audiences at massive scale. While not new to security pros — cybercriminals and unscrupulous competitors have been using bots for years to undermine websites — their use in mass influence operations (the 2016 US presidential election, for one) is novel and their imitation of human-like behaviors is as effective as it is off-putting.[5] When viewed as a whole, they appear as swarms of accounts due to the attributes, activity, and audiences they all share (see Figure 1). They mimic user behavior by posting on popular topics to appear benign as they gain influence and evade detection (see Figure 2).[6] Given the growth and range of botnets today, any negative press story could be the catalyst that thrusts your organization into the spotlight, whether the story is real or not.
- **Financial gain as a motive will attract even more cybercriminals and crime syndicates.** Election rigging and political upheaval aren't the only goals for attackers launching cyber influence campaigns. Attackers weaponize social media for financial gain. They use influence operations

to move stock markets for their benefit and curate dormant botnets patiently waiting for the right corporate crisis to go viral and strike. Financial gain is the bread and butter of cybercriminals. For years, they would short a company's stock, launch a devastating DDoS attack on its online channel, and sit back and reap the rewards when the stock dropped. Reputational and brand attacks can now take the place of the DDoS attack.

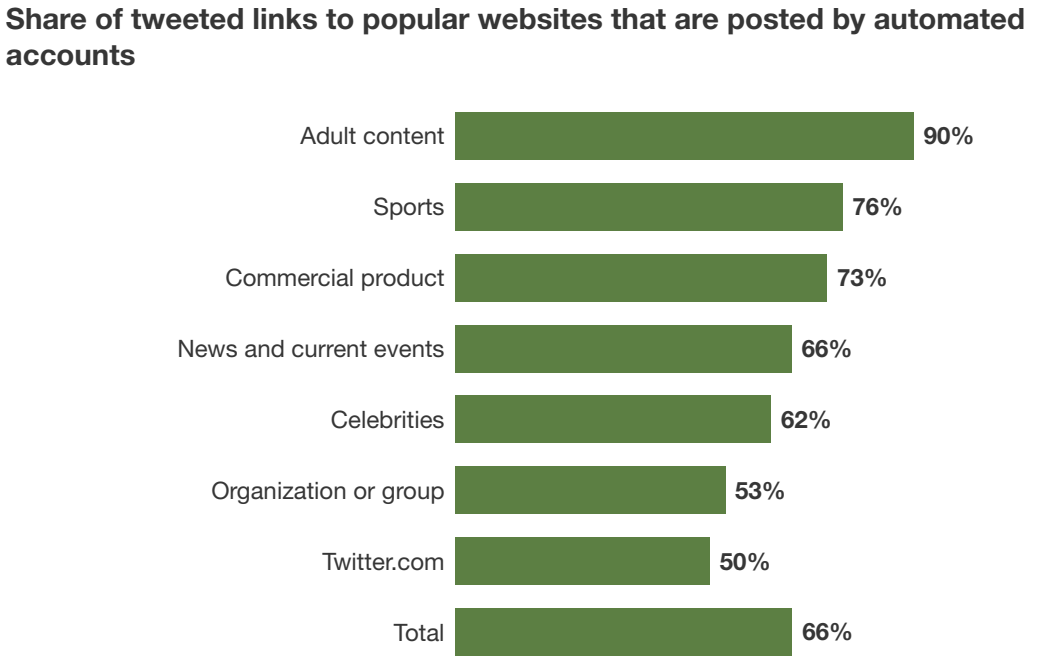
› **AI makes this even easier for attackers and opens up new avenues for extortion.** A human threat actor can't operate at the same scale and speed as AI-powered toolkits and botnets. Machine learning techniques can mine large amounts of data and monitor tweets and posts to create personalized botnet campaigns. Data like that harvested from Facebook by Cambridge Analytica, and the publicly available voter data used by AggregateIQ to target voters, make it possible for nation-states and hacktivists to target specific segments with AI-generated fake news.[7] With face-swapping technology and voice synthesis, attackers can create realistic looking videos and audio featuring powerful figures such as politicians, civic leaders, or entertainers.[8] AI can also generate text for social media, blog posts, and fake news sites. It will be possible to launch a digital extortion attack of fake news to discredit a company, its executives, or its products, thereby holding the company hostage.

FIGURE 1 The Hidden Linkages Of Social Botnets That Feed Fake News



Source: Zignal Labs dashboard

FIGURE 2 Bots Use Popular Topics And Sites To Imitate Real User Behavior And Evade Detection



Source: Stefan Wojcik, Solomon Messing, Aaron Smith, Lee Rainie, and Paul Hitlin, "Bots in the Twittersphere," Pew Research Center, April 9, 2018

Your Cybersecurity Playbook Isn't Ready To Combat Influence Attacks, But It Needs To Be

Public sentiment and perception shift at incredible speed. The 24-hour news cycle, prevalence of social media, and hyperconnectivity accelerate the amount and speed at which individuals ingest information on a global basis. While this is a boon for people and businesses, it's also a threat to organizations that require visibility to create value. Every business leader and organization is a potential target of disinformation campaigns that use social media to incite calls to action against that entity. While on a small scale this may seem as nothing more than a nuisance, when tens of thousands of bots and purchased troll farms aim cohesively at a target, the speed and power of the data flow can be staggering. S&R pros are used to protecting networks, apps, and data from direct attack; now they will have to adapt their cybersecurity strategy, architecture, and processes to protect the firm from these novel attacks. As you do so, realize that:

› **Exploiting sentiment and damaging reputation is as harmful as malware.** These attacks never "touch" your infrastructure. Instead they use channels like social media and negative press to amplify and distort information about your company; they aim to take minor events and shape a narrative, turning events into a major crisis that consumes time, attention, and capital. S&R pros need to broaden their definition of cyberattack if they're going to help business leaders prepare and combat these attacks.

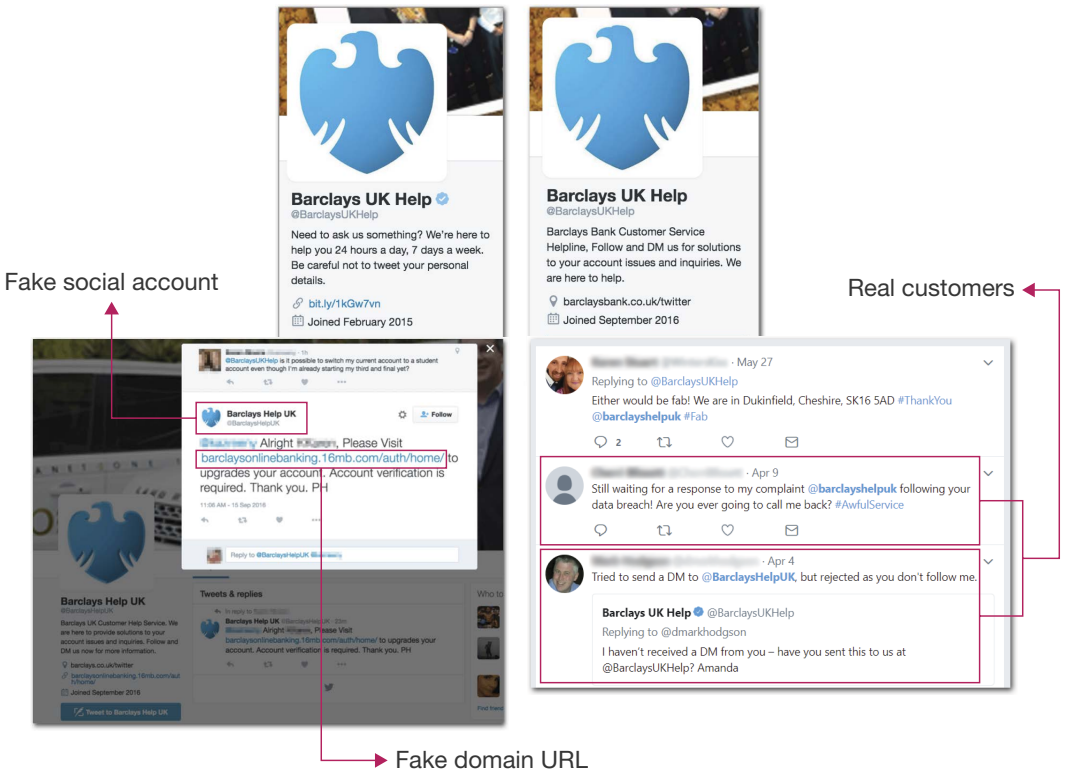
- **Fear and emotion stifle facts and reason.** Daily news, immediate insights, and the proliferation of content add to the threat. One study from MarketingDive.com found that thirty-eight percent of Americans said they get their news from social media but only 37% view it as a trustworthy source, compared to 70% that feel printed news, including magazines, is credible. An overwhelming 85% said they use Facebook as their top news source on social.[9] The nature of social media — that it's delivered without searching for it, on a near-real-time basis — means that even though the source is less reputable, it reaches the individual and shapes their opinions faster than more trusted, but slower, news outlets. This data shows that the majority of the public essentially reacts to "news" via their gut feeling, or their emotions. Fear and emotional responses based on possibly, or in some cases, likely, bogus reporting can be extremely threatening.

  The attacker's message spreads in feeds, while the actual explanation gets ignored or summarized because firms fail to understand that the distribution of information has become more important than the content itself. S&R pros will need to challenge business leaders and marketers who want to combat these attacks with facts and reason, and explain how these attacks exploit an audience's willingness to believe something is true. Put an actionable plan in place, just as with cyberthreats or hacking. S&R leaders need to have a clear and decisive action plan in place for when, not if, these attacks occur.

- **Such attacks impersonate, take over, and extort your brand and key executives.** Social media accounts are compromised at an alarming rate. But unlike most common cyberattacks, your adversaries don't even need access to your social accounts to wreak havoc — they can create their own versions: Attackers stole Barclays' customer accounts and data by creating lookalike accounts to phish real customers on Twitter (see Figure 3).[10] With the recent emergence of social botnets, cybercriminals have new ways to scam and extort your brand — like threatening to unleash a torrent of negative posts with a bot army unless the company pays a hefty Bitcoin ransom.[11]

- **The tech giants won't be coming to the rescue anytime soon.** Facebook, Google, Microsoft (including LinkedIn), and Twitter are four of the major tech companies facing the brunt of the influence threats. It's fair to say they've made some strides to shore up their porous security efforts in the wake of the Cambridge Analytica scandal (failings which we were calling out for years prior!), but they still have a long way to go.[12] You can't wait for the big boys to lead the way and protect you. Even if they manage to tame the geopolitical and nation-state threats, that still leaves a host of other ways influence operations and botnets can target organizations.[13] If your company values its customers' faith and trust, move quickly and decisively to show customers what plans you have for defending their data and privacy from these types of campaigns.

FIGURE 3 Rogue Accounts, Impersonations, And Likeness Hijacking Run Rampant On Digital Channels



Source: Proofpoint

Prepare For Psychological Warfare Outside The Wire With Zero Trust

Zero Trust forces security and risk pros to challenge underlying trust assumptions in their architecture and processes. When we take a Zero Trust security posture, we assume attackers have already infiltrated our network and malicious insiders are routinely pilfering sensitive data. This is why Zero Trust demands continuous monitoring and maintaining of situational intelligence of the environment. With Zero Trust, we are always on the lookout for the tell-tale signs of breach or intrusion in progress so we can react to contain and stop it before it becomes a devastating event.

Now we must apply the same Zero Trust principles to protect our external digital footprint. Given the accelerated migration of digital assets and infrastructure that now reside beyond the network and on third-party environments, S&R pros have to assume the same posture for attacks that originate outside the wire. We should expect that targeted cyber influence campaigns could be launched at a moment's notice or are already underway. A Zero Trust mindset outside the wire starts with the recognition of the threat that computational propaganda and influence operations represents to all organizations. Security

leaders need to develop specific response plans that address the nature of the attack, the distribution channels that must be included, the motivations of the attacker, and how to reconnect with customers that have lost faith or trust in the brand.

Understand Influence Attack Tactics, Techniques, And Procedures (TTPs)

To protect your organization, you must first understand how cyber influence attacks work, how your adversaries can use them against you, and the common targets and motivation behind them. This should sound familiar: It's the same process for consuming, analyzing, and adapting to internal and external cyberthreat intelligence, and this expertise is one of the critical reasons why security pros need to take a prominent role in combatting influence attacks. However, there are some important differences. Security pros must:

- **Treat social sentiment as critical threat intel.** Remember, cyber influence attacks don't extend your perimeter — they circumvent it altogether. Every leader, business, and organization that exists in today's marketplace has some form of social media presence and an external online perception that drive both business and public understanding of the organization.[14] It's now a key part of doing business, which means it's an extension of your team's boundary or perimeter. Security pros must pay attention to how social sentiment and perception shifts and how adversaries could weaponize it.[15] In fact, NopSec finds Twitter data instrumental in its annual vulnerability risk management reports, discovering a strong correlation between the number of tweets and the threat CVEs pose.[16] Your team should consider methods and strategies to actively detect and combat malicious campaigns that can be launched at the drop of a hat.
- **Evaluate social media as an important attack vector.** Most cybersecurity professionals are concerned with malware and exploit packs that criminals use to hack systems and networks via technical means. While app vulnerabilities and weaknesses are the most common attack vectors, and exploits of these apps is a powerful threat, they're not the only ones. A Twitter campaign coordinated and planned against your business can be just as effective at damaging the bottom line. A single tweet or video is just a problem, but 100,000 of those, with the right language calibrated and coordinated at a singular target, can eviscerate a business at a shocking pace. Malicious actors and threat groups in Russia, China, and Iran have been hiring trolls and Twitter bots and agents focused solely on retweeting and swaying public perception of a target. That target could easily be your business or its leadership and can undermine your reputation and customers' trust.
- **Familiarize yourself with computational propaganda and psychographics.** Mathematicians and political science researchers have found they can use mathematical formulas to analyze populations, separating them into thousands of subgroups according to defining characteristics like religion, political beliefs, and taste in TV shows. Other algorithms segment by heated issues, categorizing users by influences and followers, pinpointing those most susceptible to suggestion. Malicious actors, propagandizers, and influencers can use similar algorithms to hone messaging that influences those users, deploying it through social media channels in hopes of altering targets'

behavior with content guaranteed to work, without regard for truth.[17] If this seems farfetched, an individual recently used online advertising on a social media site to guarantee that the CEO of a firm he was interested in working for would see his résumé. Security and risk pros need to work with and learn about targeted advertising to get a better sense for what is possible here.

- **Recognize that video and bot farms are a real threat.** One of the biggest digital ad frauds ever perpetuated was identified by the firm White Ops. During this hack, cybercriminals made over $3 million a day by manipulating valid video ads and click-tracking systems. The White Ops team dubbed this manipulation of video as Ad Fraud Komanda or AFK13.[18] In this scenario, hackers created thousands of related domains and hundreds of thousands of URLs that appeared to belong to real publishers, from ESPN to Vogue. With faked domain registrations, the malicious actors were able to trick algorithms that decided where the most profitable ads would go into buying their fraudulent web space. AFK13 actors then invested heavily in a click-bot farm (over half a million bots) that could fire faked traffic at those ads, thereby driving their illicit revenue via the pay-per-click system they had exploited. With other bots "watching" those bogus video ads over 300 million times per day, and with an average payout of $13.04 per thousand for their faked video views, the fraudsters made millions.
- **Recognize how attackers turn user-generated data into its own cyberweapon.** Users and consumers generate vast troves of data on all manner of topics, including what they think and how they respond to ideas, arguments, marketing material, and, in some cases, controversial topics — literally tens of thousands of expressions of thought, belief, and cognizance are generated every second on Facebook, Google, Reddit, and Twitter. All of those digitized data points are collected and stored, analyzed and processed. Additionally, much of that data is available commercially or via open source repositories to anyone with sufficient computing power to take advantage of it. The same data your firm uses to engage with customers can help adversaries craft more-effective spear phishing campaigns. Attackers can track click rates too.
- **Prepare for fake videos that will make your CEO look criminal.** Using algorithms to swap faces, match voices, and create fake videos with people saying or doing things they never did, also poses a risk to organizations. When faceswapping techniques debuted, it was in the form of advanced algorithms developed by a global network of academics participating in collaborative research. Within 500 days, free apps became available to make your own face swap videos on home computers. All attackers have to do now is create fake videos of your CEO or corporate spokesperson engaging in unethical, immoral, or unpopular behavior, and then spread the fake video to cause lasting damage to your enterprise — and damage to the individual's life.

Deploy A Digital Risk Protection Strategy With A Zero Trust Mindset

Understanding the scope of the threat that these soft tactics pose is a key first step since they're still so new and unfamiliar. In the ethereal space of digital marketing, knowledge of online exposure and user sentiment is extreme power. The more insight and knowledge your team has, the better your

defenses will be. Just as your team strategizes tactics and technologies to mitigate traditional security threats, follow the same tenets as you design and deploy a digital risk protection (DRP) strategy.[19] Make sure you can execute the necessary actions at each of the following DRP steps:

1. **Map out your entire digital footprint, assets, and exposures online.** Employ some of the basic tenets of Zero Trust by knowing what actually poses a risk to your organization, within or beyond your network and infrastructure. Use account discovery, social media insight, and other tools to detail and understand the totality of the avenues of assets that might cause an issue for your team. DRP vendors like Censys, Cybersprint, Qadium, and RiskIQ specialize in digital footprint mapping and will help you identify, visualize, and track all publicly accessible assets and infrastructure.[20] Don't trust that you have a total baseline of assets and items that might be a potential avenue of threat; verify that reality and constantly monitor it.
2. **Monitor channels for indicators of attack, compromise, and abuse.** Applying Zero Trust outside the wire means you can't ever assume your social media accounts and mobile apps are secure or accurate until you can prove it. To put it simply, trust nothing. This requires that you actively track your known digital assets as well as new rogue or lookalike accounts spoofing your brand or personnel. Look for DRP tools with robust data collection and analytics, and those that can support your team with ongoing protection and remediation (e.g., CyberInt, Digital Shadows, IntSights, Proofpoint, SafeGuard Cyber, and ZeroFOX).[21] If you believe you're at risk of botnet-driven influence attacks, a social bot intelligence tool like Zignal Labs will help your team keep tabs on active and dormant social botnets that present a threat to your organization or industry. If you have an indication that sentiment or news might be bashing your brand, act as if you were hacked.
3. **Mitigate risk with prepared response plans and automated remediation.** Computational propaganda and influence attacks are new threats, meaning your team likely has little to no experience in handling them. Extend your defensive perimeter beyond the DMZ by preparing your team to actively and accurately monitor, manage, and defend against these threats. Whiteboard sessions and tabletop exercises are effective ways of planning for actions that will occur in the future. Do these exercises on a regular cadence to ensure that your team is ready to react when the time comes. Additionally, consider employing tools that build formalized playbooks for your team so that everyone operates on the same page when responding to disinformation campaigns.

What It Means

Counterpsyops Will Become A Key Responsibility For Cybersecurity

When thinking about nation-state threats, most S&R pros typically think of the massive hacking operations such as operation Olympic Games where the US and Israel combined to hack centrifuges against Iran, or the stories of Russian malware targeting banking institutions.[22] That still happens, but it's only a tool in the quiver of nation-state organizations. Those same actors and threat groups have extended and innovated their operational capabilities well beyond the scope of just banking and

government hacks. Those same threat teams have come to understand that they can simply kill a target softly through prolonged news and media campaigns that slowly undermine the perception of an organization. A death by a thousand cuts is still death. In the future, S&R pros should expect:

- **Brand asset security to rise as a critical security priority.** Voice, visual, and video content are easier and cheaper to manipulate every year. As this trend continues, brand counterfeits and persona impersonations get more realistic and difficult to discern. Security teams will have to pick up the mantle to help their companies ensure the authenticity of their organization's brand assets and public figures and their associated digital content and presence.
- **Industry-accepted psyops training courses and certificates to emerge.** As psychological operations (psyops) becomes a more prevalent activity, security leaders and staff will seek out formalized training to ensure they're equipped with the right resources and knowledge to tackle influence threats, and a cadre of traditional and new cybersecurity vendors and consultants will be happy to oblige.
- **CISOs to more closely align with their CMOs for brand security.** For years, we have discussed how critical it is for CISOs to align with the CIO; privacy has made it critical for CISOs to align much more closely with the CMO, and the need for band security will make this unique relationship even more critical. Marketing owns the brand itself, but CISO and their team will have responsibility to make sure this message is consistent and reliable and any brand elements that are online are secure.
- **The psyops industry to turn corporate.** Corporate monetization of psyops-type programs is already happening, and it's growing. In the future, you will see companies with big-time marketing presences formalize their psyops activities to promote their own products and brands online, to counter cybercriminal psyops, and (more discreetly) to disparage the competition. For example, vendors like Babel Street and VizSense work with and advise marketing teams on how to develop and deploy these tactics. Some firms will likely step over ethical lines and seek out less scrupulous "marketing agencies" that are willing to live on the dark side of this business.
- **Traditional cybersecurity vendors to jump on the bandwagon.** Threat intelligence, DRP, and other security vendors will develop counter psyops offerings to tackle all elements of cyber influence threats and match a skills and capabilities gap. Expect the array of related security products and services to include targeted bot intelligence and detection, verification and validation for controlled digital assets, incident response and remediation services, and counterbotnets to reduce the reach and muffle the messaging of adversary botnets.
- **VR/AR adoption will enhance psyops effects exponentially.** Mass adoption of virtual reality and augmented reality (VR/AR) are still far off, but when they do take hold, cyber influence operations will have an even bigger impact. The immersive experience of these technologies will provide new opportunities to hijack and manipulate human senses. It's too early to predict exactly what shape the threats will take, but consider adding it to your threat modeling if you're in an industry that will be an early adopter.

Supplemental Material

Companies That Contributed To The Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

CyberInt

Cybersprint

Proofpoint

RiskIQ

SafeGuard Cyber

ZeroFOX

Zignal Labs

Endnotes

[1] In fact, intangible assets such as intellectual property, good will, proprietary "know-how," user base, customer experience, brand, and reputation account for 87% of the net worth of the S&P 500.

See the Forrester report "GRC Vision 2017-2022: Customer Demands Escalate As Regulators Falter."

Source: Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," Computation Propaganda Research Project (http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf).

[2] Source: Peter Dizikes, "Study: On Twitter, false news travels faster than true stories," MIT News, March 8, 2018 (https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308).

[3] For example, imagine that a small bank in the midwestern United States makes loans, takes deposits, and operates day-to-day as banks do. Perhaps that bank advertises through a website that becomes associated with a controversial figure, or makes a political donation to a candidate that's caught up in a scandal. A threat actor that's never heard of this small bank contracts a bot farm that has access to tens of thousands of hacked and available Twitter feeds, Facebook pages, and other profiles. The malicious actor uses that network, making the bank a trending topic of controversy. Smaller organizations do not possess the resilience or diversity to weather a storm of attention like this, especially if they lose customer trust and faith in their business.

[4] Source: "How bots amplify hoaxes and propaganda on social media," Recode, August 2, 2018 (https://www.recode.net/2018/8/2/17636264/josh-ginsberg-zignal-bot-recode-decode).

[5] Source: Gabe O'Connor and Avie Schneider, "How Russian Twitter Bots Pumped Out Fake News During The 2016 Election," NPR, April 3, 2017 (https://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election).

[6] Source: Stefan Wojcik, Solomon Messing, Aaron Smith, and Paul Hitlin, "Bots in the Twittersphere," Pew Research Center, April 9, 2018 (http://www.pewinternet.org/2018/04/09/bots-in-the-twittersphere/).

[7] Source: Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," The Guardian, March 17, 2018 (https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election).

[8] Source: William Welser, "Fake news 2.0: AI will soon be able to mimic any human voice," Wired UK, January 8, 2018 (https://www.wired.co.uk/article/fake-voices-will-become-worryingly-accurate).

[9] Source: David Kirkpatrick, "Study: Fake news undermines trust in social, digital outlets more than traditional media," Marketing Dive, November 1, 2017 (https://www.marketingdive.com/news/study-fake-news-undermines-trust-in-social-digital-outlets-more-than-trad/509742/).

[10] In addition to account takeovers, attackers may also impersonate a brand to launch fake promotions (e.g., a Facebook page impersonating Delta Air Lines that promised $5,000 and free first class tickets), steal customer data, promote hashtags laden with malicious posts during major events like the Olympics or Academy Awards (AKA "hashtag hijacking"), or anger customers (e.g., a spoofed Facebook profile impersonating Target's customer service account, which trolled customers online). See the Forrester report "Four Ways Cybercriminals Exploit Social Media."

[11] Source: Joseph Cox, "Scammers Threaten to Review Bomb a Travel Company Unless it Pays Ransom," Motherboard, August 29, 2018 (https://motherboard.vice.com/en_us/article/8xbpdb/scammers-review-bomb-twitter-bots-instagram-fake-reviews-cheapair-std-company).

[12] Forrester has been publishing research social media threats since 2012. In May 2016, we called social media the "new cyberweapon of choice" for cybercriminals. In that research, we specifically pointed to the security failures of major social networks — Facebook, LinkedIn, and Twitter — and throw into question the reliability and accuracy of their fake account estimations. Source: Nick Hayes, "Facebook, LinkedIn, Twitter: The New Cyberweapons Of Choice," Forrester Blogs, May 18, 2016 (https://go.forrester.com/blogs/16-05-18-facebook_linkedin_twitter_the_new_cyberweapons_of_choice/).

See the Forrester report "Manage The Risks Of Social Media."

[13] Social media is a cybercriminal gold mine. The ways in which they can take advantage of these channels and their users in different phases of the cyberattack is essentially limitless. See the Forrester report "Four Ways Cybercriminals Exploit Social Media."

[14] A firm's digital footprint encompasses every touchpoint, mention, and affiliation that's linked to the company. Given the large number of social networks, mobile apps, and websites where this activity can occur, the number of associated corporate accounts, sites, apps, and ads can easily rise into the thousands for large organizations. See the Forrester report "The Forrester Wave™: Digital Risk Monitoring, Q3 2016."

[15] The vast majority of companies' net worth no longer comes from physical assets (e.g., real estate, industrial equipment, cash) but from assets that are less easily quantified (e.g., brand health, innovation, customer experience, data). In fact, in 1975, intangible assets accounted for approximately 17% of the S&P 500's market value; today, that percentage has risen to more than 87%. For this reason, company performance is now reliant on a positive perception of the quality, desirability, and overall worth of these assets — and more detrimental when this perception falters. See the Forrester report "Brand Resilience: Understanding Risk Managers' Key Role In Protecting Company Reputation."

[16] Source: Jordan Dominguez, "CVSS Score," NopSec blog, May 17, 2016 (https://www.nopsec.com/blog/malware-analysis-moving-beyond-cvss-score/).

[17] Source: Kate Conger and Charlie Savage, "How Fake Influence Campaigns on Facebook Lured Real People," The New York Times, August 2, 2018 (https://www.nytimes.com/2018/08/02/technology/facebook-fake-accounts.html).

[18] Source: "The biggest online advertising fraud in history, and how blockchain can make ad fraud history," The AdEx Blog, June 21, 2017 (https://medium.com/the-adex-blog/the-biggest-online-advertising-fraud-in-history-and-how-blockchain-can-make-ad-fraud-history-7ba9f10e238).

[19] "Digital risk" is your firm's exposure to damaging activity on external digital channels that directly impact your business, brand, or people. In essence, it's the business risk from digital channels you don't, and often can't, fully control. Therefore, digital risk events are unique in that, in order to protect them, you have to rely on and interact with the social networks, ISPs, and other external entities that hold that control. Since you never have full control, you must shift your own security and protection objectives from prevention to detection and response. See the Forrester report "Assess Your Digital Risk Protection Maturity."

[20] Digital footprint mapping tools track firms' digital assets and infrastructure. These solutions help security pros discover and manage systems, devices, and other externally facing digital assets. They provide an attacker's view of these assets, including valid and invalid web domains and IP addresses, as well as digital and physical infrastructure and access points. See the Forrester report "New Tech: Digital Risk Protection, Q2 2018."

[21] DRP solutions offer rapid event detection and remediation capabilities so companies can fix issues before bad actors exploit them (e.g., sensitive data publicly exposed due to misconfigured Amazon S3 buckets, impersonated social media accounts, or phishing websites) and to limit the effects of successful attacks when they occur. See the Forrester report "The Forrester New Wave™: Digital Risk Protection, Q3 2018."

[22] Source: David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," The New York Times, June 1, 2012 (https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.