DOWNLOAD PDF BUILD YOUR OWN ARMY OF WEB BOTS WITHIN 24 HOURS (ARMY OF WEB BOTS SERIES, 1)

Chapter 1 : How Twitter Bots and Trump Fans Made #ReleaseTheMemo Go Viral - POLITICO Magazine

Build Your Own Army of Web Bots Within 24 Hours (Army of Web Bots Series, 1) (v. 1) by Monica Lamb (Author).

What follows is a post-mortem on those digital sieges, which featured a mix of new and old-but-effective attack methods. Junk traffic sent by a DNS amplification attack. There was one indication that a story I published just hours before the attacks began â€" about a service for mass-registering domain names used for malware, spam and other dodgy business â€" may have struck a nerve: In one of the attacks, all of the assailing systems were instructed to load that particular story many times per second. The first DDoS campaigns consisted of several hundred systems repeatedly requesting image-heavy pages on my site. The traffic signatures from the attack strongly suggest the involvement of two Dirt Jumper progeny: Image courtesy Prolexic Pandora is the latest in the Dirt Jumper family, and features four different attack methods. According to Prolexic, the one used against KrebsOnSecurity. They claim 1, Pandora bots are enough to bring Russian search engine giant yandex. Prolexic said more than 1, Pandora-infected bots were used in the assault on my site. The third sortie was by far the largest, and employed a very effective method known as a DNS reflection attack. In such attacks, the perpetrators are able to leverage unmanaged DNS servers on the Web to create huge traffic floods. Typically, DNS servers only provide services to machines within a trusted domain. But DNS reflection attacks rely on consumer and business routers equipped with DNS servers that are mis configured to accept queries from anywhere on the Web. That way, when the DNS servers respond, they reply to the spoofed target address. Indeed, I used this tool to check dozens of Internet addresses that were seen sending my site replies to spoofed DNS lookups, and all were home to open recursive DNS servers. Open recursive DNS servers leveraged in the attack. The bad guys also can craft DNS queries so that the responses are much bigger than the requests; they do this by taking advantage of an extension to the DNS protocol that enables large DNS messages. For example, an attacker could compose a DNS request of less than bytes, prompting a response that is times as large. And this is exactly the approach they used with the DNS attacks on my site. The DDoS problem overall is not going away and seems to be worsening. And a proliferation of consumer-grade and SOHO routers deployed by ISPs that are unmanaged all but ensures the raw firepower for reflected DNS attacks will remain a nuisance for some time. You can follow any comments to this entry through the RSS 2. Both comments and pings are currently closed.

DOWNLOAD PDF BUILD YOUR OWN ARMY OF WEB BOTS WITHIN 24 HOURS (ARMY OF WEB BOTS SERIES, 1)

Chapter 2 : - Browse books by ISBN starting with - Used books at Biblio

Build Your Own Army of Web Bots Within 24 Hours (Army of Web Bots Series, 1) by Monica Lamb. Published February by Authorhouse. Written in English.

Everything you need to start a life of cybercrime is just a few clicks and many more dollars away. Building successful malware is an expensive business. It involves putting together teams of developers, coordinating an army of fraudsters to convert ill-gotten gains to hard currency without pointing a digital arrow right back to you. So the biggest names in financial botnetsâ€”Zeus, Carberp, Citadel, and SpyEye, to name a fewâ€”have all at one point or another decided to shift gears from fraud rings to crimeware vendors, selling their wares to whoever can afford them. In the process, these big botnet platforms have created a whole ecosystem of software and services in an underground market catering to criminals without the skills to build it themselves. They even come with full technical support to help you get up and running. The customers of these services often plan more for the short term than the long game played by the big cyber-crime rings. They have very different goals. Botnet infrastructures can be applied in lots of ways for different sorts of profitâ€”cash, information, or political gain. There are many ways to make money off botnets beyond outright theft, such as using them to steal advertising clicks, generate spam e-mails for a paying client, or renting out bots for denial-of-service attacks. And the same basic principles used to distribute botnets have been creeping up in more targeted attacks to steal intellectual property or to spread the malware used in the recent "wiper" attack on South Korean banks and broadcasters. So how easy is it to get into the botnet business? Well, Ars decided to find out. Given the surprising availability of botnet building blocks online, I set out to build a shopping list to understand how everything is bought and sold within this black market. All I had to do was paste in "botnet" in Cyrillic, and I was on my way down the rabbit hole. That may be the scariest lesson here. With absolutely no budget for bitcoins, I got my start with some help from Max Goncharov, a security researcher for Trend Micro who specializes in following the Russian underground marketplaces for online fraud services. Goncharov detailed some of these services in a paper published late last year and presented during this press road show. Of course, that price is for a particular type of botnet. It also assumes total noob-hood. For those seeking to do something a little less overtly criminal than stealing credit card numbers or committing wire fraud, there are less expensive options. With a little sweat equity, you can pull off a workable botnet for a fraction of that price. With my rough estimate in place, it was time to actually start some research of my own. The marketplace of bad ideas The "underground" forums do more than just give would-be criminals access to a level of service that might make some enterprise software companies look bad. On these barely underground sites, hacker wares are made available to anyone willing to pay. Current versions of Zeus and SpyEye botnet software are for sale, or you can find the last version cracked by someone for cheap or free. Many of the sites run under the thin veneer of "security" discussion boards. These are largely the small and medium businesses of cybercrime, following a well-worn approach to making money. When a piece of malware like a botnet lands on thousands of PCs, "it may hit the radar of an antivirus company pretty quickly," Percoco noted. That means time and money spent on finding new victims, deploying patches and updates, paying for new exploits, and generally continuing the game of "whack-a-mole" with antivirus companies and other organizationsâ€”as the mole.

DOWNLOAD PDF BUILD YOUR OWN ARMY OF WEB BOTS WITHIN 24 HOURS (ARMY OF WEB BOTS SERIES, 1)

Chapter 3 : A beginnerâ€™s guide to building botnetsâ€”with little assembly required | Ars Technica

[PDF]Free Build Your Own Army Of Web Bots Within 24 Hours download Book Build Your Own Army Of Web Bots Within 24 racedaydvl.com InformationWeek, serving the information.

Continue to article content On Tuesday morningâ€”the day after the House Intelligence Committee voted along partisan lines to send Rep. The vote marked the culmination of a targeted, day information operation that was amplified by computational propaganda techniques and aimed to change both public perceptions and the behavior of American lawmakers. By the time the memo got to the president, its release was a forgone conclusionâ€” even before he had read it. Story Continued Below This bears repeating: The analysis below, conducted by our team from the social media intelligence group New Media Frontier, shows that the releasethememo campaign was fueled by, and likely originated from, computational propaganda. It is critical that we understand how this was done and what it means for the future of American democracy. Promoters of releasethememo rapidly began mocking the idea that they are Russian bots. There are even entirely new accounts set up to tweet that they are not Russian bots promoting releasethememo, even though their only content is about releasing the supposed memo. But this back and forth masks the real point. It is computational propagandaâ€”meaning artificially amplified and targeted for a specific purposeâ€”and it dominated political discussions in the United States for days. The releasethememo campaign came out of nowhere. The frenzy of activity spurred lawmakers and the White House to release the Nunes memo, which critics say is a purposeful misrepresentation of classified intelligence meant to discredit the Russia probe and protect the president. You can unsubscribe at any time. And this, ultimately, is what everyone has been missing in the past 14 months about the use of social media to spread disinformation. And they can be surprisingly effective. None of them, to this point, were talking about releasethememoâ€”the hashtag, that is. The hashtag originated with Twitter user underthemoraine at 3: The tweet tags the president, realDonaldTrump. He has a history of tweeting about trending conservative media topicsâ€”Antifa, BlueLivesMatter, boycotting the NFL, social media filtering out conservative views, the climate change "hoax," special counsel Robert Mueller. Moraine has few followers 74 at last count and is not particularly influential. However, his account is followed by several accounts that are probable bots as well as by the verified account of the Michigan Republican Party MIGOP, which first used releasethememo at 5: It was registered in , tweeting only a handful of times between July and November mostly against President Barack Obama and in favor of the GOP. Then the account goes dormant until June â€”the period that was identified by former FBI Director James Comey as the beginning of the most intense phase of Russian operations to interfere in the U. The frequency of tweets builds from a few a week to a few a day. By October 11, there are dozens of posts a day, including YouTube videos, tweets to political officials and influencers and media personalities, and lots of replies to posts by the Trump team and related journalists. All of these topics were promoted by Russian disinformation campaigns. There is little content promoting Trump; it is almost entirely attacking Clinton. Since the revival of the account, there are more than 32, tweets and repliesâ€”about 66 tweets per day, plus a similar amount of likes. Why would a bot account follow some nobody in Michigan? KARYN follows hundreds of such accounts, plus conservative media, and a lot of other bots. Back to the afternoon of January This was, primarily, what the Well account didâ€”retweet and reply to accounts with hashtags included, marking them into messaging campaigns. Well is engaging and directing traffic to a specific group of accounts on specific discussions. These accounts often have short shelf lives, appearing as needed and disappearing when their usefulness has passed or once flagged by Twitter. Though we have confirmed her identity, we will not use it here, as she does not. The twitter ID is the same as an email listed on a linked-in account for a woman in South Carolina, an early primary state, who is a nutritionist and hemp-oil promoter. The profile photo was changed from an anonymous meme to a picture of the woman with Trump at a political rally after she was accused of being a bot for promoting the hashtag. A woman with the same name was recently interviewed by a German newspaper for a profile on Trump supporters. So, this

seems to be the account of a real person voluntarily and quite deliberately participating in the effort to amplify the reach of releasethememo. In the 24 months since the account was established, Queen has tweeted 47, timesâ€”about 65 times per day, so about the same rate as the active bot. She has tweeted releasethememo hundreds of times in a few days. Each list includes at least a few bots. Some bots are amplifiersâ€”in the simplest form, they automatically follow accounts that follow them, and retweet tweets from those accounts sometimes, other parameters such as keywords are factored in. It is an element of automation. The rest is about network, echo chamber, fake influence and amplification. Popping up a little further down the line, around 6 p. For the first few hours, only fringe accounts promote releasethememo. There is little chance an organic or incidental community, even of friends or acquaintances, would look this way online so holistically, tweeting together in such tight intervals. Several of the accounts involved in the initial promotion of this hashtag have subsequently been restricted or suspended by Twitter. Online data analysts said many accounts used to promote the hashtag were recently created, with more being created and disappearing after the hashtag appeared. Thousands still had the default profile photos. Cross-reference this analysis and inputs from things like the Hamilton68 dashboard, and you can see releasethememo is carried forward by automated accounts overnight after it begins to trend. It continued to do so from its appearance until the memo was released. The volume and noise matterâ€”and so does the targeting. A key function of the accounts discussed above is that they tweet at key influencers with these messaging campaignsâ€”media personalities, far-right brand names, and elected officials who might pick up the info or hashtag and legitimize it by repeating it. A few active verified accounts, including KamVTVâ€”an account that often appears as the first verified amplifier of bot and far-right contentâ€”and scottpresler, picked up the hashtag, and others retweeted tweets sent to them from sketchy accounts. Any one of these targets could see the hashtag in their mentions, replies and quoted-tweets. For example, Zeldin tweeted at 4: He used the hashtag transparency. In the 4 hours after that tweet, there were more than tweets targeting him with the hashtag releasethememo. Before midnight, King, Meadows and Gaetz had all tweeted releasethememo; so had Laura Ingraham, a massively influential conservative media personality with 2 million followers. Each time an influential verified account used the hashtag, it was rapidly promoted by a vast network of accounts. From its appearance until midnight, releasethememo was used more than , times. The hashtag had become the organizing framework for multiple stories and lanes of activity, focusing them into one column, which got a big boost from right-stream media and twitter personalities. Some, like Breitbart, would argue this volume is representative of the outpouring of grass-roots support for the topic. But compare this time period to other recent significant events. This is because the hashtag benefited from computational promotion already built into the system. It was used to target lawmakers who would play a role in releasing the memoâ€”lawmakers who argued that there was public pressure to release the memo. Up until the time of the vote, Republican members of the House Intelligence Committee were collectively targeted with releasethememo messages over , times. By the time Speaker of the House Paul Ryan spoke in favor of releasing the memo, he had been targeted with more than , messages about it. Trump, whom the Washington Post reported was swayed by the opinions of some of the congressmen listed above, was targeted more than a million times. Fox News personality Sean Hannity, said to speak daily with Trump, was targeted , times and became a significant promoter of the hashtag. What does it all mean? There is no leadership. No one is building awareness of how these automated influence campaigns are being used against us. For example, by using it to achieve a political goal like releasing the Nunes memo. Social media platforms have worked diligently to make us believe they had no idea this was happening, or that they are working to expose and correct the problem. But the algorithms work exactly as they are supposed toâ€”in one aspect, by reinforcing your own beliefs without challenging them, and in another, by creating perceptions of popularity that are intentionally false and coercive. If the Twitter analysis referred to by the Daily Beast has been accurately conveyed by the source, there should be many questions. How are they determining influence? Did Twitter know the origins of the releasethememo campaign when it suspended some apparently many of the accounts involved? A recent analysis from DFRLab mapped out how modern Russian propaganda is highly effective

because so many diverse messaging elements are so highly integrated. This gets at a deeper issue: What is happening on social media is very real; it is not passive; and it is information warfare. Alt-right groups and Russian disinformation campaigns are often indistinguishable since their goals often overlap. But what really matters is the tools that these groups use to achieve their goals: Computational propaganda serves to distort the political process and amplify fringe views in ways that no previous communication technology could. The challenge we still have in unraveling what happened in is how hard it is to pry the Russian components apart from those built by the far- and alt-rightâ€”they flex and fight together, and that alone should tell us something. As should the fact that there is a lesser far-left architecture that is coming into its own as part of this machine. And they all play into the same destructive narrative against the American mind. What matters is that someone is trying to manipulate us, tech companies are proving hopelessly unable or unwilling to police the bad actors manipulating their platforms, and politicians are either clueless about what to do about computational propaganda orâ€”in the case of releasethememoâ€”are using it to achieve their goals. Americans are on their own. And, yes, that also reinforces the narrative the Russians have been pushing since Would that a leader would step into this breech, and challenge the advancing victory of the bots and the cynical people behind them. McKew is an expert on information warfare and the narrative architect at New Media Frontier. This article tagged under:

Chapter 4 : Triple DDoS vs. KrebsOnSecurity â€” Krebs on Security

Build Your Own Army of Web Bots Within 24 Hours (Army of Web Bots Series, 1) buy Satellite News is not financially supported by Best Brains or any other entity. It is a labor of love, paid for out of our own pockets.

Chapter 5 : Kings of Chaos :: Build Your Army, Conquer Your Enemies, Become a King of Chaos!

Programmers and nonprogrammers will be able to use this book as a plain English step-by-step guide with detailed instructions about installing, customizing, and using Web Bots, Artificial Intelligence, Speech Synthesis, and Voice Recognition for Web site interactivity.