Independent Submission
Internet Draft
Intended status: Informational
Expires: January 8, 2020

D. Lazanski
Last Press Label
July 2019

An Internet for Users Again
draft-lazanski-smart-users-internet-00.txt

Status of this Memo

Copyright Notice

Abstract

RFC 3552 introduces a threat model that does not include endpoint security. In the fifteen years since RFC 3552 security issues and cyber attacks have increased, especially on the endpoint. This document proposes a new approach to Internet cyber security protocol development that focuses on the user of the Internet, namely those who use the endpoint and are the most vulnerable to attacks.

Table of Contents

1. Introduction

Data breaches are on the rise: personal data is stolen and often leaked or sold on a never-before-seen scale. The truth is that malware and ransomware attacks impact the most vulnerable in our global societies today. But the key to better privacy is better security and cyber defence. And better cybersecurity, ultimately, results in even better privacy. However, even though IETF attendees are privacy-focused, policy and design decisions taken by the IETF have radically changed the architecture of the Internet, arguably without due consideration to cyber defence implications or outcomes. In recent years, this has obsoleted many systems, technologies and programmes which use Internet protocols for prevention, detection and mitigation of cyber attacks. RFC 7258 established that "Pervasive Monitoring" is an attack on privacy that needs to be mitigated where possible. Furthermore, RFC 3552 assumes that the endpoints involved in a communications exchange have not been compromised, but that the attacker has near complete control over the network between the endpoints rather than the endpoints themselves. These assumptions have led to a focus on communications security and the development of protocols that place this kind of security above all else. Ironically - or coincidentally - as the development of these protocols have taken place over the last several decades, there has been and continues to be a sharp rise in cyber attacks. The Internet threat model in RFC 3552 does not even mention that the greatest threat to the Internet is the growing scale and variety of cyber attacks against all types of endpoints that is resulting in significant data breaches. This now needs to change.

2. A History of Data Breaches

A data breach is an incident where data is inadvertently exposed in a vulnerable system, usually due to insufficient access controls or security weaknesses in the software.[1] In the first six months of 2018 alone, Gemalto reported that there were 945 data breaches resulting in 4.5 billion records being compromised.[2] This section describes some recent cyber attacks on the Internet which led to data breaches.

In October 2013, Adobe announced that hackers had stolen nearly 3 million encrypted customer credit card details and the IDs and encrypted passwords of 35 million customers.[3]

In December of 2013, the retailer Target announced that 40 million credit card records and personal details for a further 70 million customers had been compromised. A report from Verizon indicated that

after one week, 86% of passwords used by Target had been cracked and Verizon's security consultants were able to move about with complete freedom on Target's internal network.[4]

In May 2014, eBay notified 145 million users to change their passwords following a cyber attack that compromised encrypted passwords, customer names, email addresses, mailing addresses, phone numbers and dates of birth.[5]

In July 2015, a commercial website that enabled extramarital affairs (called Ashley Madison) was breached; a month later, more than 25GB of company data, including user details, was leaked. The ethics and impact on human rights of this breach are particularly notable, as it resulted in at least one confirmed suicide.[6]

In 2016, Uber was breached, giving hackers access to the names, email addresses and phone numbers of 57 million riders and drivers. 600,000 US drivers had their names and license plate numbers stolen. The current assessment is that other personal data, including trip location history, credit card details, social security numbers and dates of birth were not downloaded. [7]

Also, in August of 2016, Dropbox was hacked to release over 68 million user email addresses and passwords onto the Internet. [8]

In March 2018, as part of a coding review, Google uncovered a coding glitch that potentially exposed the personal data of up to 500,000 Google Plus users, including their names, email addresses, occupations, genders and ages.[9] Google could not confirm which users were affected by the security flaw as they keep API log data for only two weeks (and, presumably, log data analysis was lacking or insufficient to detect the breach as it was happening).

In May 2018, Twitter advised all 330 million of its users to change their passwords after a software exposed them in plaintext. [10]

Additionally, in September 2018, British Airways announced that personal and financial details of up to 380,000 customers who had booked flights over a 16-day period had been stolen. This breach was traced to a rogue script that had been installed on the third-party payment supplier used by British Airways.[11]

Also in September 2018, Facebook suffered its worst security breach ever; the exploitation of several simultaneous software bugs gave login access to as many as 50 million accounts.[12] April 2019, a 146GB data set containing over 540 million Facebook records were

found exposed on AWS servers, as two third-party companies had collected Facebook data on their own servers.[13]

In November 2018, 500 million Marriott International customers had their details stolen in an ongoing breach since 2014. Approximately 327 million hotel guests had a combination of name, address, phone number, email address, passport number, date of birth, gender and arrival/departure information stolen.[14]

In January 2019, the personal data of more than 3500 people living with HIV in Singapore was leaked in Singapore, allegedly by an insider with access to sensitive records.[15]

In February 2019, a file containing 2.2 billion compromised usernames and passwords was found on the dark web. This 600GB file was a collation of previous data breaches, truly demonstrating the scale and severity of the data breach and cyber defence problem in totality.[16]

And these are only a handful of breaches that have been made public. So many more go unreported in the public. Data breaches are one of the singular most important issue in cybersecurity today. In IBM's 13th "Cost of a DataBreach" study found that the global average cost of a data breach in 2018 was $3.86 million.[17] That is the average cost of one - not many -data breaches.

It is unthinkable and unrealistic that any revised Internet threat model does not highlight the large and ongoing threat from data breaches, whatever their cause. Threat actors are making full use of the Internet technology that allows them to hide on endpoints and perform such large data hacks that mostly go undetected.

Internet security research and technical development must accept the reality of all the security issues in the Internet ecosystem. Decisions being made in the name of privacy are sometimes leading to larger inadvertent security and privacy losses.

3. Botnets

A botnet is a string of connected computers used, in this case, to perform a malicious function against an end user, organisation or series of users.[18] Though computers working together to increase computing power for functions does not constitute a botnet in itself (and is used often in data centres for chat rooms or email services, for example) botnets are a specifically used for malicious intent.

There have been a number of recent, high profile botnet attacks and only a few will be described here as examples.

In 2000, EarthLink Spammer sent 1.25 million phishing emails over a year and made $3 million in profits by using fake websites and domain names to accomplish this. Subsequently the spammer was convicted and Earthlink won $25 million in damages.[19]

Created in 2007, Cutwail was the biggest botnet on the Internet by 2009 by number of infected computers or hosts sending email. It was sending 51 million emails every minute.[20] By 2010, however, it started a DDoS attack to nearly 300 major sites including PayPal and US federal agencies. By 2013 it was the botnet to use for sending spam, but over time its use declined through targeted attempts to take it offline as well as the expiration of email addresses. Though not as popular and sending far less than it once did, Cutwail still sends spam to this day.[21]

A more recent botnet was the centre of one of the biggest outages of the Internet network. The Mirai botnet was first identified in 2016. The Mirai botnet as well as variants infect Internet of Things devices and those infected devices scan the Internet for IP addresses of other Internet of Things devices, thus creating a multiplication of IoT devices which are infected. Though the bot still exists in various forms, the most serious attack took place on 21 October 2016 when the Domain Name System (DNS) provider Dyn was attacked by DDoS using a coordinated system of infected IoT devices. Much of the Internet was unreachable after three attacks occurred during the day. Though eventually resolved on that day, the sheer size and scale of the attack is still viewed as one of the biggest attacks on the Internet to this day.[22]

According to Kaspersky Labs, there were just over 15,000 botnet attacks in 2018.[23] Worryingly, of those attacks, approximately 40 percent were new in both type and the target. Again, as IoT devices increase and as networks expand coverage and ability to handle even more devices and data, it is likely that botnet attacks will continue to be seen on such a scale.

4. Emerging Threats

Older methods of cyber attacks are still happening and causing breaches, as endpoint security remains incomplete and not up to date. Servers remain unpatched and vulnerable and client devices become legacy or unsupported, to name just a few issues. In parallel, new categories of attacks are emerging.

Software updates are a new attacked vector. In March 2019, Kaspersky uncovered the ShadowHammer supply-chain attack which injected malicious code into the ASUS Live Update Utility. This attack involved signing malicious code using stolen certificates and was estimated to have affected half a million users.[24] As a result of the ShadowHammer attack, public focus turned to how and what could be the point of infection. Suggestions were that the IP addresses could have been the point of origin of the attack while others suggested that the malware itself was dormant and inactive until a certain update triggered the malware.

In July 2019, Godlua became the first publicly known malware to use DNS-over-HTTPS to avoid DNS-based malware protection security systems. [25]

Though attacks on individual consumers have dropped by nearly 40 percent, due to the fact that attacking one person is largely not financially viable, but attacks on business organisations have increased year on year.[26] Ransomware is on the rise, motivated by economic gain and the ever increasing weaknesses in endpoints. Malware is freely available and the vulnerable attack point of an endpoint can be found. Botnets are increasing in size and scale as well as ease of use.

There are other emerging threats that require more research to collate fully; this section is a starting point.

5. An Internet For Users Again

Many endpoints are vulnerable; CLESS begins a much needed research programme to demonstrate what capabilities and what limitations can be expected at the endpoint and from a variety of types of endpoints.[27] Endpoints have changed over the last 10 years, but assumptions about endpoints in the IETF hasn't changed in that time.

Even the user is not in full control of what happens on their endpoint much of the time and what security protections apply to their own data; a model where the Internet is user-centric would give more control to the user. The user is both the home Internet citizen and the organisation administrator seeking to protect against data breaches; both need the power to control where their data goes and choose their security protections. So while endpoints are the focus now, does the Internet need to be user-centric in the future? Won't that give users even more assured privacy?

ATT&CK versions of methods, when categorised by type, show that endpoint methods of compromise are increasing faster than network

attacks.[28][29] This may be due to more variety in endpoints, substandard security in many endpoints or the difficulty of attacking a network compared to an endpoint. Whatever the reason, the logical conclusion is that the current Internet design is not stopping cyber attacks. Perhaps a fresh approach is required.

As more power and control has shifted to endpoints - and even to only a select few applications on endpoints - fewer and fewer network-based security solutions have been effective and attacks have increased. The diagram above shows the proliferation of attacks on endpoints increase over a 3 and a half year timescale while network and physical attacks remain largely unchanged. Whether this is correlation or causation requires thorough research, essential to changing the existing threat model approach from its current approach.

The existing Internet Threat Model of RFC3552 makes the general assumption that end-systems have not been compromised and that while end-systems are difficult to protect against compromise, protocol design can help minimise the damage.[30] Revisiting this general assumption in the light of the magnitude of an increase in data breaches and their subsequent negative results is a good starting point for a new Threat Model which can result in protocol design that helps mitigate end-system compromise.

6. Security Considerations

This document proposes a new way of thinking about developing Internet security protocols and does not create, extend or modify any protocols. The intent is to initiate discussion.

7. IANA Considerations

Upon publication this document has no required IANA considerations.

8. Conclusions

The Threat Model indeed needs revisiting and changing, because cyber defence threats and attacks are increasing, yet the responsibility to help mitigate these threats and attacks is largely unrecognised in the IETF community - as of yet. These threats and attacks should be given the seriousness they deserve.

Further, it is imperative that new conclusions and recommendations from a revisited threat model are backed up by research, case studies and experience - rather than bold assertions. Research and

evidence is important to achieve effective security; unsubstantiated guesswork is not.

While this draft does not claim to hold all the answers or all of the research questions, it highlights the importance that any threat model must be based in evidence about data breaches. This draft initiates a much needed discussion which, as mentioned, is that it is time to think, discuss and research what a new Threat Model - with all security issues of note - included.

At this stage, we merely insist that the possibility of an Internet for users - for the user to be in control of mitigations against a new and more substantive threat model - is not blatantly disregarded. An endpoint without user control doesn't work; user control must be permitted in future threat models. For most users and current as well as future deployments, it will be the best way to protect personal data and ensure privacy.

9. References

9.1. Normative References

No normative references.

9.2. Informative References

[1]https://haveibeenpwned.com/FAQs/

[2]https://www.cbronline.com/news/global-data-breaches-2018

[3]https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/

[4]https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

[5]https://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5

[6]See https://digitalguardian.com/blog/timeline-ashley-madison-hack for a timeline of the breach.

[7]https://us.norton.com/internetsecurity-emerging-threats-uber-breach-57-million.html

[8]https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

[9]https://www.experian.com/blogs/ask-experian/google-data-breach-what-you-need-to-know/

[10]https://www.theverge.com/2018/5/3/17316684/twitter-password-bug-security-flaw-exposed-change-now

[11] https://medium.com/asecuritysite-when-bob-met-alice/the-british-airways-hack-javascript-weakness-pin-pointed-through-time-lining-dd0c2dbc7b50

[12]https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

[13]https://www.databreachtoday.co.uk/millions-facebook-records-found-unsecured-on-aws-a-12337

[14]https://www.bbc.co.uk/news/technology-46401890

[15]https://www.straitstimes.com/singapore/2400-singaporeans-affected-by-data-leak-contacted-by-moh

[16] https://mobilesyrup.com/2019/01/31/collection-2-data-breach-600gb-leaked-emails-passwords/

[17]https://securitytoday.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx

[18]https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

[19] https://www.bizjournals.com/atlanta/stories/2002/07/22/story4.html

[20]https://www.whiteops.com/blog/9-of-the-most-notable-botnets

[21]https://www.wired.co.uk/article/infoporn-rise-and-fall-of-uks-biggest-spammer

[22]https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained

[23]https://securelist.com/bots-and-botnets-in-2018/90091/

[24]https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

[25]https://www.techspot.com/news/80791-meet-godlua-first-known-malware-leverages-dns-over.html

[26]https://blog.malwarebytes.com/cybercrime/2019/04/labs-cybercrime-tactics-and-techniques-report-finds-businesses-hit-with-235-percent-more-threats-in-q1/

[27]https://datatracker.ietf.org/doc/draft-taddei-smart-cless-introduction/

[28]Pastor, Antonio."Applying AI to Protect 5G Control Traffic", ETSI Security Week, 19 June 2019, ETSI, Sophia Antipolis, France.

[29]https://info.vectra.ai/hubfs/no_index/compliance/cb_mitre_082318.pdf

[30]RFC3552, 2004, Section 3 Internet Threat Model: "In general, we assume that the end-systems engaging in a protocol exchange have not themselves been compromised. It is, however, possible to design protocols which minimize the extent of the damage done under these circumstances."

10. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Dominique Lazanski
Last Press Label
London, UK

Phone: +447783431555
Email: dml@lastpresslabel.com