One Thing Leads to Another: Credential Based Privilege Escalation

Peter Snyder and Chris Kanich
University of Illinois at Chicago
Chicago, Illinois, USA
{psnyde2,ckanich}@uic.edu

Abstract

A user's primary email account, in addition to being an easy point of contact in our online world, is increasingly being used as a single point of failure for all web security. Features like unlimited message storage, numerous weak password reset features and economically enticing spoils (in the form of financial accounts or personal photos) all add up to an environment where overthrowing someone's life via their primary email account is increasingly likely and damaging. We describe an attack we call credential based privilege escalation, and a methodology to evaluate this attack's potential for user harm at web scale. In a study of over 9,000 users we find that, unsurprisingly, access to a vast number of online accounts can be gained by breaking into a user's primary email account (even without knowing the email account's password), but even then the monetizable value in a typical account is relatively low. We also describe future directions in understanding both the technical and human aspects of credential based privilege escalation.

Categories and Subject Descriptors

H.3.5 [**Information Storage and Retrieval**]: On-line Information Services; J.m [**Computer Applications**]: Miscellaneous; K.4.4 [**Computers and Society**]: Electronic Commerce

Keywords

web security; web privacy

General Terms

security; privacy

1. INTRODUCTION

At the heart of most cybercrime is unauthorized access: attackers are able to transfer information, computation, and economic value (from e.g. credit cards or bank accounts) from victims to themselves. The value proposition for attackers is composed of two parts: gaining unauthorized access to systems or accounts, and extracting the valuable information from those stores of value. Traditional analysis of cybercrime primarily focuses on the criminal efforts as a sort of one-two punch: first gain access to a large store of e.g. credit card numbers from a retailer, then somehow monetize that information, either through selling to a third party or performing fraudulent transactions.

While the unauthorized access portion of a sophisticated cybercrime attack is likely to consist of multiple break-ins chained together—for instance an unpatched web server allows a remote exploit, after which a database server is breached from inside a corporate firewall—these attacks are typically carried out by humans and rely on exploiting the unique configuration of the network at hand. However, the current web ecosystem lends itself to a different type of multi-stage attack which is much more easily automated, in an attack we call credential based privilege escalation.

"Privilege escalation," as traditionally defined, allows attackers with some foothold into a system to access more resources than they were intended. Typically, this is enabled by some flaw in the software installed on the machine. However, in credential based privilege escalation, multiple factors combine to allow the attacker to gain additional privileges. These factors are largely not purely technical problems and many have a human component: passwords shared between accounts, sites that email passwords in plain text, or even account reset capabilities which are amenable to social engineering.

There is no doubt that stealing the credentials to one database server housing credit card records is far more lucrative than breaking into several trivial online accounts. However, through any of the above weaknesses, even an account as inane as a discussion forum or a mobile videogame has the potential to allow an attacker to escalate his privilege, perhaps by re-using that password to log in to the user's email account, after which the user might be able to take over several other possibly lucrative accounts. This issue is exacerbated by how email accounts have become central to users' online lives: a large portion of online accounts defer all security to the email account through "password reset" features, thus ensuring that if an attacker wants carte blanche to impersonate someone online, they need only compromise that person's email account. Indeed, the hacking of technology journalist Mat Honan showed how complete and damaging this type of privilege escalation can be if the attacker's goal is vandalism rather than personal gain [7].

CODASPY'15, March 2–4, 2015, San Antonio, Texas, USA.
ACM 978-1-4503-3191-3/15/03.
http://dx.doi.org/10.1145/2699026.2699127.

Due to the homogeneity and popularity of many modern online accounts, the risk that an attack like this could be automated by a motivated attacker could greatly endanger user safety on the web.

Understanding the extent to which credential based privilege escalation is possible is an important first step to determining what steps can be taken to mitigate it on the web. As this is both a social and technical problem, approaches to defending against it must consider both the human victims and attackers, as well as the extent of the damage poor system design choices can have. Here we describe our approach to investigating both users' perceptions of these threats, along with the true extent of the damage they might cause.

2. RELATED WORK

Much work has been done documenting how cyber criminals monetize account credentials and in what volumes they are able to do so. Thomas and Martin[4] documented the diverse and specialized systems that cyber criminals use for buying, selling and monetizing a wide variety of stolen pieces of information, including online credentials. Similarly, Franklin et al[5] measured the types of information bought and sold on black market forums. They found that that the majority of traded data related to credit cards, with less than 1 percent of data being username / password values.

Others have found that the underground market for account credentials is not as active as had been previously claimed. In investigating who bore the greatest burden from financial cyber crime, Florencio and Herley [4] found that while forums were active with offers to buy and sell stolen credentials, the actual number of documented completed trades was very low, and advertised prices were heavily discounted, possibly indicating a difficulty in monetizing stolen credentials.

Other work has been done into how cyber criminals are able to acquire the account credentials they hope to monitize. Moore and Clayton[9] found that between 280,000 and 560,000 individuals have credentials stolen through phishing attacks each year, and the FBI has documented the millions of dollars stolen through credentials stolen from the Zeus Botnet[3] from [1]. Krebs [8] also found that criminals extract passwords and other account credentials where possible from breached machines. Holz et al. [6] point out that credentials are also commonly stolen from shared machines and public terminals, where many people input their credentials into a malicious devices.

3. METHODOLOGY

To evaluate credential based account escalation, we built a prototype "account theft audit" tool. The operation of our tool has been approved by the IRB of our institution. As it appears to the user, our tool provides an analysis of their personal email accounts and gives them feedback, both on how much those accounts are reported to be worth on the cybercriminal underground, as well as which accounts might be easily accessed via an attacker who gains access to their primary email account.

To build our prototype, we combined three components: first, we gather empirical information about how much access to different accounts is worth to cybercriminals. Then, we performed a survey of many popular web properties to create signatures for both their welcome email messages and their password reset policies. Finally, we combine these information sources in our account theft audit tool through a web application. This process is a win-win for users and researchers, as users get immediate feedback about the security and value of their account, and we gain another data point regarding how prevalent risk due to credential based privilege escalation is on the web.

3.1 Underground Value

Assessing value in underground markets is a difficult proposition: by their very nature, successful underground markets shield their participants and their no doubt illegal activities from view. Even so, cybercrime researchers have been able to find price lists for several different types of accounts online [2]. While these price lists are certainly suspect, the fact that these accounts are being offered for sale when many of them can have their password reset via the email address associated with the account shows that credential based privilege escalation can allow a cybercriminal with access to a set of email accounts to amplify their earnings by selling both the email account and the accounts within it piecemeal on the cybercriminal underground.

3.2 Web Account Survey

We include the price information in the account theft audit mostly as supplementary information for the user: far more important for us is the web account survey which shows how much an attacker's access can be amplified via shared password or email-based password resets. We combined a manual analysis of English language websites which were popular hacking targets in underground markets with a list of websites that send passwords via plain text in email [10]. This information allows us to both warn a user when a shared password might be revealed to an attacker via a password reminder email, and when an attacker could amplify their access via a password reset request to a compromised email account.

3.3 Web Tool Prototype

Finally, we combine these information sources with a web-based email account analysis platform of our own design. For a previous project, we built an infrastructure which allows users to opt in to a web based experiment which gives our server temporary access to a subset of the capabilities of their Google account - specifically, their Gmail account. Importantly, this access is explicitly temporary, does not include any knowledge of the credentials needed to log in to the account, and can be revoked by the user immediately via a Google web page if they so choose (rather than being mediated by our server).

Our prototype performs a series of searches against their gmail account for messages sent from a list of popular or insecure web accounts. The prototype can scan a gmail account with over 4 gigabytes of email for these accounts in under 45 seconds, and gives the user instant feedback about both the progress of the scan and progressively adds new accounts to the report as they are found.

4. PRELIMINARY RESULTS

Through our underground market reconnaissance we have pricing information on seven different accounts, and we track account existence for 1,475 accounts. We've had 9,026 users

try the service and opt in to having their information included in the study.

From the data we have collected, the average account price is $14.17, and the maximum account price seen was $40.05. While these prices are most likely not completely accurate in the cybercriminal underground, this average shows that several of the tracked accounts are very popular with both cybercriminals and users of our tool, showing that vulnerability to credential based privilege escalation is quite common among our study participants.

While we only have limited results now, we wish to explore several other angles to this problem which we present next in Section 5.

5. FUTURE WORK

Our prototype is currently deployed and actively collecting data. However, we have several angles we wish to explore in this space using this study and tool. While our current approach focuses on the extent to which credential based privilege escalation enables access amplification for cybercriminals, the human component is just as interesting: can an account theft audit tool, which gives users an extremely personal reminder of both how important their email account is, improve security by giving users a "teachable moment" about protecting their accounts? Exploring this hypothesis via either value to cybercriminals or other proxies for account value like number of messages, account age, or number of accounts created via this email address might enable service providers to impress better security practices on their users.

Our current model of privilege escalation is built around password reset via email and plaintext passwords, either those stored in the account, or those sent by poorly implemented services. As seen in both the Mat Honan example and the August 2014 iCloud photo compromise, many other vectors exist for privilege escalation via social or technical means - in the Honan example it was social engineering using credit card number fragments, and in the iCloud example, one likely culprit was a non-rate-limited security question prompt for account reset.

These two privilege escalation angles each present new challenges: in the first example, evaluating the ease with which an attacker can socially engineer a customer service representative would allow us to form a more complete model of what a motivated but non-expert cybercriminal would be able to accomplish. In the second example, a more complete model of how to take over an account, beyond simple password reset via email, must be considered as well. Understanding each of these attack vectors will bring us closer to a more systematic and complete understanding how cybercriminals perform account takeover.

6. ACKNOWLEDGEMENTS

This work was supported by National Science Foundation grant CNS 1351058.

7. REFERENCES

[1] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., and Savage, S. Measuring the cost of cybercrime. In *WEIS* (2012).

[2] Danchev, D. Hacked origin, uplay, hulu plus, netflix, spotify, skype, twitter, instagram, tumblr, freelancer accounts offered for sale. `http://www.webroot.com/blog/2013/06/07/hacked-origin-uplay-hulu-plus-netflix-spotify-skype-twitter-instagram-tumblr-freelancer-accounts-offered-for-sale/`, 2013.

[3] Federal Bureau of Investigation. International cooperation disrupts multi-country cyber theft ring. `http://www.fbi.gov/news/pressrel/press-releases/international-cooperation-disrupts-multi-country-cyber-theft-ring`, October 2010.

[4] Florencio, D., and Herley, C. Is everything we know about password stealing wrong? *Security & Privacy, IEEE 10*, 6 (2012), 63–69.

[5] Franklin, J., Perrig, A., Paxson, V., and Savage, S. An inquiry into the nature and causes of the wealth of internet miscreants. In *ACM conference on Computer and communications security* (2007), pp. 375–388.

[6] Holz, T., Engelberth, M., and Freiling, F. *Learning more about the underground economy: A case-study of keyloggers and dropzones*. Springer, 2009.

[7] Honan, M. How apple and amazon security flaws led to my epic hacking. `http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/`, Aug 2012.

[8] Krebs, B. The scrap value of a hacked pc. `http://voices.washingtonpost.com/securityfix/2009/05/the_scrap_value_of_a_hacked_pc.html`, May 2009.

[9] Moore, T., and Clayton, R. Examining the impact of website take-down on phishing. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (2007), ACM, pp. 1–13.

[10] van Kloeten, O., and Tabachnik, I. Plain text offenders. `http://plaintextoffenders.com/`, 2012.

8. REFERENCES

[1] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., and Savage, S. Measuring the cost of cybercrime. In *WEIS* (2012).

[2] Danchev, D. Hacked origin, uplay, hulu plus, netflix, spotify, skype, twitter, instagram, tumblr, freelancer accounts offered for sale. `http://www.webroot.com/blog/2013/06/07/hacked-origin-uplay-hulu-plus-netflix-spotify-skype-twitter-instagram-tumblr-freelancer-accounts-offered-for-sale/`, 2013.

[3] Federal Bureau of Investigation. International cooperation disrupts multi-country cyber theft ring. `http://www.fbi.gov/news/pressrel/press-releases/international-cooperation-disrupts-multi-country-cyber-theft-ring`, October 2010.

[4] Florencio, D., and Herley, C. Is everything we know about password stealing wrong? *Security & Privacy, IEEE 10*, 6 (2012), 63–69.

[5] Franklin, J., Perrig, A., Paxson, V., and Savage, S. An inquiry into the nature and causes of the wealth of internet miscreants. In *ACM conference on Computer and communications security* (2007), pp. 375–388.

[6] Holz, T., Engelberth, M., and Freiling, F. *Learning more about the underground economy: A case-study of keyloggers and dropzones*. Springer, 2009.

[7] Honan, M. How apple and amazon security flaws led to my epic hacking. `http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/`, Aug 2012.

[8] Krebs, B. The scrap value of a hacked pc. `http://voices.washingtonpost.com/securityfix/2009/05/the_scrap_value_of_a_hacked_pc.html`, May 2009.

[9] Moore, T., and Clayton, R. Examining the impact of website take-down on phishing. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (2007), ACM, pp. 1–13.

[10] van Kloeten, O., and Tabachnik, I. Plain text offenders. `http://plaintextoffenders.com/`, 2012.