ROPEMAKER:
Stop Trying to Make it Happen;
ROPEMAKER is Not Going to Happen

NullBites
College Drop Out
CISSP & CEH Holder
0x00sec IRC Lurker
Email: nullbites@protonmail.com*

August 31, 2017

Abstract

ROPEMAKER is an "exploit" that takes advantage of the fact that it is possible to modify what is visible in an email after it has been delivered by using remote content features in modern e-mail clients.

Despite this both "messages" are still present in the email text, so it is possible under most corporate policies to filter these out or to alert on the fact that employees are being prepositioned to sell secrets.

Does **ROPEMAKER** pose a threat to users in actual environments?

nah...

*Thanks to r_netsec and the other hooligans at 0x00sec

Rejected Titles:

ROPEMAKER: an inch to hang by, a mile ROPE

ROPEMAKER: the diamonds for swine, except the diamonds are broken glass from when you were roughhousing with your cousin and he threw you though a sliding glass door.

ROPEMAKER: The Scientology of Exploits

ROPEMAKER: hacking by people who use CISSP & CEH as a title on their resume

Introduction:

Ropemaker appears to be a vector for making phishing campaigns more effective against end users. The faulty primise in this line of thinking is that:

1. Users are hardened Phishing investigators that need a SHA512 gpg signature for every email they receive(hyperbole).

2. Current phishing techniques are ineffective because users are using and validating security measures(sarcasm)

$\therefore$ We need to use edge case HTML + CSS features in our phishing emails to fool them

The truth of the matter is that there are significantly easier methods for forging valid looking emails (especially with HTML[1]). Given that mimecast®is a security company that focuses on email: I am surprised that this isn't written on a wall somewhere. Another commonly forgotten potential phishing principal is that there are always going to be the "click everything" users that don't need the effort of a custom HTML and CSS emails. There are, even after massive amounts of money spent on phishing training, users that believe some Nigerian Prince is going to give them money as long as they fill out this RTF document and send it back.

An even better example is[2] an email that contains an image that looks like a windows XP error prompt; Complete with "Ignore" & "Cancel" buttons. This dastardly and cunning pop-up imitation would then link to an exploit kit and you get to steal my nana's retirement checks. :(

Given a sufficiently large enough pool of users[3]: there will be clicks. This is a statement of fact.
This is a fact consistently exploited by adversaries.

So then what is the answer to the phishing problem? How do we stop our users from clicking on all this 8/8 gr8 b8?

Well... it's not this.

[1] Users Don't expect functionality from an email, so most "pretty" emails sent by companies are extremely replicatable by simply copying and modifying the source; Just like making your own website in 2004!

[2] Thanks Grandma

[3] 5+ maybe?

What is ROPEMAKER?

The following is a non-comprehensive list of things that ROPEMAKER is not:
1. A 0-day
8. a 1337 0-D@y
6. a 31337 0-day
7. A well named new technique
5. A new class of injection vulnerability
3. A vulnerability in literally any meaningful way
0. A pretty neat party trick for people who own email servers
9. Totally not a shameless advertising campaign.

The Following is a non-comprehensive list of things that ROPEMAKER is:
1. Not An 0-day
8. Not an 1337 0-D@y
6. Not na 31337 0-day
7. A conjunction of two unrelated words trying way too hard to copy the "NSA naming convention"
5. Not A new class of injection vulnerability
3. Not A vulnerability in literally any meaningful way
0. A pretty lame party trick for people who own email servers
9. A shameless advertising campaign? - this is still up for debate

Does ROPEMAKER Pose A Risk to my Company?

This depends on your definition of risk. Pull out your CISSP hats everyone[4]. There are dozens of Risk Management Frameworks we can chose from. Many of these frameworks are great examples of how to assess, categorize, rate and identify risk. Using these tool we can understand and implement controls to mitigate... God, no, wait... what the hell am I talking about!?! I need raw lye for my tongue.

I need Edward Norton, Brad Pit, and meatloaf to grant me forgiveness for this subservience to "The Mathmatics of Death". Oh woe is this RMF, oh woe is this NIST standard. I have become John's shriveled heart. Deadened by the cold and heartless view of computer security as a subset of risk management. I'm a red teamer. Why the hell am I complementing RMFs like they do anything besides what gets the money moved for the blue team?

Let's look at this shit from Red's perspective. From the perspective of he or she who would actually use this.

[4]It should be in your ass, I know mine is :)

A Red Team Operator's Perspective

This is bullshit, the whole thing is bullshit, why are we allowing this crap on our precious /r/netsec? Why are we putting up with what is obviously corporate garbage meant to shill a service that weakly tests something any competent RT operator should be able to do by him/herself?

It's because for some CISOs all they want is to buy a magic "Risk Control" box or service[5] that mitigates all of the risk so he can sit back, take it easy, and coast just a few short years into that sweet, sweet retirement money.

...

Okay, enough with the borderline nihilist cynicism of my own industry - lets discus something useful. Scale.

Scale is a huge and oft unconsidered multiplier of risk in security. As much as I knock risk management frameworks, it is a useful gauge of how much work to do and in what areas. So for scale we have a multiplicative factor for risk. The larger the scale - the more likely it is that pentesters and quality assurance testers miss bugs that red then pick up, and could leverage as vulns. With that in mind; How do we apply that concept of scale to the email system of a large company?

Or even more broadly how do we apply this to users as a whole?

We don't. It's that simple

For years it has been preached to build security systems under the assumption of assumed compromise. The solution to email security is to not trust your users. It's that simple. Build a resilient network that segments the users in a safe manner, verifies need-to-know, and correctly implements access controls.

"Bro that is way to difficult. You mean we have to hire competent people? Do you know how hard that is?"

Get bent loser, that's just the way it works. You can spend all the money you want on services and assessments, but nothing beats a solid network configuration[6].

[5] Preferably both

[6] Except APTs maybe, but the risk of that is signifigantly lower then your average crook. And that is the guy who you should worry about.

Conclusion

Get fucked