



INFORMATION BULLETIN

Orange County Intelligence Assessment Center

(U//FOUO) Criminal Use of E-mail Filters to Monitor and Divert Communications

22 February 2017

(U) Overview

(U//FOUO) The Orange County Intelligence Assessment Center (OCIAAC) has received reporting indicating cybercriminals are manipulating e-mail filters as a means to monitor and divert e-mail communications. Cybercriminals may use malicious e-mail filters to:

- (U//FOUO) Monitor victims' e-mail after malware removal and password changes
- (U//FOUO) Monitor victims' e-mail without continuously logging in to victim accounts
- (U) Divert e-mails that might alert the victim of a system compromise

(U) Application of E-mail Filters

(U//FOUO) Cybercriminals must first gain access to victim's e-mail accounts in order to implement malicious e-mail filtering. Access might be gained by:

- (U) Password guessing
- (U) Password cracking/brute force attacks
- (U) Eliciting credentials through the use of fake websites and forms
- (U) Eliciting credentials via phone calls
- (U) Sending the victim credential-stealing malware
- (U) Exploiting documents where passwords are written down

(U//FOUO) Cybercriminals might employ this tactic in a variety of crimes and surveillance efforts, which might include:

- (U//FOUO) Stalking and cyberstalking
- (U//FOUO) Corporate, industrial, military, and economic espionage
- (U//FOUO) Tax fraud
- (U//FOUO) Mortgage fraud
- (U//FOUO) Wire transfer fraud
- (U//FOUO) Identity theft

(U) E-mail Filtering

(U) E-mail filtering is an e-mail organizational tool which allows users to label, archive, favorite, delete, or automatically forward e-mails.

(U) The word "filter" is often used interchangeably with the word "rule".

(U) Source: Gmail

This information should be considered **UNCLASSIFIED // FOR OFFICIAL USE ONLY** unless otherwise noted and contains information that may be exempt from public release under the Freedom of Information Act (5 USC 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with US Department of Homeland Security policies and is not to be released to the media, public or other personnel who do not have a valid "need-to-know" and shall not be distributed beyond the original addressees without prior authorization of the originator. Receipt acknowledges a commitment to comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information. If you have any questions or need additional information, please contact the OCIAAC.

To report suspicious activity, submit a tip or lead at www.OCIAC.ca.gov or call 714-289-3949



(U) Incidents

(U//FOUO) Examples of incidents by which criminals used e-mail filters to facilitate crimes include:

(U//FOUO) Use of Really Simple Syndication (RSS): In late 2016, an Orange County-based critical infrastructure organization was targeted in a Business E-mail Compromise (BEC) scam why which a cybercriminal compromised a Chief Financial Officer’s e-mail account. While impersonating the CFO in e-mail correspondence, the cybercriminal requested wire transfers to unauthorized bank accounts. The cybercriminal created an e-mail filter that forwarded all of the CFOs e-mails to a public RSS feed being monitored by the cybercriminal.



(U) Source: iconarchive

- **(U//FOUO) Use of “trash” mail folder:** In October 2016, an Orange County-based medical practice fell victim to a wire transfer scam. A cybercriminal compromised an accountant’s e-mail account and created an e-mail filter so that all communications from other finance personnel were sent to the accountant’s “trash” mail folder. Masquerading as the accountant, the cybercriminal requested wire transfers from finance department personnel. All responses to the cybercriminal’s requests were filtered to the “trash” folder, out of sight of the accountant, where the cybercriminal would actively wait to respond to wire transfer correspondence.



(U) Source: iconarchive

- **(U) Use of filters to evade security alerting:** According to a 2014 FireEye report, hacking group *FIN4* targeted publically traded companies and advisory firms to gain insider knowledge for trading advantage.¹ *FIN4* sent phishing e-mails to various targeted individuals. The phishing e-mails contained either Visual Basic Applications (VBA) macros or links to fake Microsoft Outlook Web Access (OWA) to steal usernames and passwords. Once *FIN4* had access to the victims’ e-mail accounts, e-mail filters were set up to automatically send any e-mails referencing “virus”, “malware” or other terms that might alert the victim to a cyber intrusion directly to the victims’ “trash” mail folder.

UNCLASSIFIED

Subject: employee making negative comments about you and the company

From: <name><compromised company's domain>

I noticed that a user named FinanceBull182 (claiming to be an employee) in an investment discussion forum posted some negative comments about the company in general (executive compensation mainly) and you in specific (overpaid and incompetent). He gave detailed instances of his disagreements, and in doing so, may have unwittingly divulged confidential company information regarding pending transactions.

I am a longtime client and I do not think that this will bode well for future business. The post generated quite a few replies, most of them agreeing with the negative statements. While I understand that the employee has the right to his opinion, perhaps he should have vented his frustrations through the appropriate channels before making his post. The link to the post is located here (it is the second one in the thread):

<http://forum.<domain>/redirect.php?url=http://<domain>%2fforum%2fequities%2f375823902%2farticle.php\par>

Could you please talk to him?

Thank you for the assistance.

<name>

(U) Sample phishing e-mail used by hacking group FIN4.

(U) Source: [FireEye](#)



(U) Mitigation




(U//FOUO) The Orange County Intelligence Assessment Center (OCIAAC) recommends auditing e-mail filters as part of the cyber incident response process. E-mail filters that may have malicious intent include:

- (U) Sending security-related e-mails to the trash or other unattended folders
- (U) Sending e-mails to suspicious e-mail addresses
- (U//FOUO) Sending e-mails to RSS feeds
- (U//FOUO) Moving e-mail correspondence containing keywords relating to sensitive topics to suspicious folders, feeds, trash, etc. (i.e. sending e-mails with keyword “SSN” or “social security” to a suspicious e-mail address)

(U//FOUO) At an organizational level, information security professionals may consider:

- (U//FOUO) Instituting a Data Loss Prevention (DLP) policy if one does not already exist
- (U//FOUO) Logging the creation of new e-mail filters across the enterprise
- (U//FOUO) Blocking the forwarding of e-mails to e-mail addresses outside the network, if in accordance with organizational policy
- (U//FOUO) Auditing e-mail rules on a regular basis to identify malicious e-mail filters and potential insider threats

(U//FOUO) Instructions for locating e-mail filters in individual Microsoft Outlook, Gmail, and Yahoo are as follows:

<p>(U) Microsoft Outlook</p> 	<ul style="list-style-type: none">• Click the “File” tab in Outlook• Click the “Manage Rules & Alerts” button
<p>(U) Gmail</p> 	<ul style="list-style-type: none">• Click the “Settings” wheel• Select “Settings” from the drop down.• Navigate to the “Filters and Blocked Addresses” tab
<p>(U) Yahoo</p> 	<ul style="list-style-type: none">• Hover over the “Settings” wheel• Select “Settings”• Click “Filters”

(U) Note: Instructions may vary on mobile applications and in versions of these products published after the publication of this document

(U) If you have any questions regarding this information bulletin, contact the OCIAAC at OCIAAC@ociac.ca.gov

(U) Tracked By:
(U) HSEC 8.3.1, HSEC 1.3.1, HSEC 1.4.2, OCIAAC I.1.C, OCIAAC III.1

¹ (U) FireEye. *Hacking the streets? FIN4 likely playing the market.* 2014 <https://www2.fireeye.com/rs/fireeye/images/rpt-fin4.pdf>
Accessed 9 February 2017.



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu