



Products (<https://www.recordedfuture.com/products/>)

Recorded Future

CREATING AN INSIGHTFUL WORLD

[Customers \(https://www.recordedfuture.com/customers/\)](https://www.recordedfuture.com)
(<https://www.recordedfuture.com>)

[Customers \(https://www.recordedfuture.com/customers/\)](https://www.recordedfuture.com/customers/)

[Resources \(https://www.recordedfuture.com/resources/\)](https://www.recordedfuture.com/resources/)

[Partners \(https://www.recordedfuture.com/partners/\)](https://www.recordedfuture.com/partners/)

[About \(https://www.recordedfuture.com/about/\)](https://www.recordedfuture.com/about/) [Blog \(https://www.recordedfuture.com/blog/\)](https://www.recordedfuture.com/blog/)

[Login \(https://www.recordedfuture.com/live/login/\)](https://www.recordedfuture.com/live/login/)

Hidden Link Analysis Reveals 92%

Posted by **Staffan** on August 11, 2015 in Cyber Threat Intelligence

[\(https://www.recordedfuture.com/category/analysis/cyber/\)](https://www.recordedfuture.com/category/analysis/cyber/)

Download the “Two Shady Men” report for free here (<http://go.recordedfuture.com/two-shady-men-report>).

Blacklists are a useful and common tool for enterprises actively looking to keep suspicious IP addresses and URLs off their network and away from their infrastructure. Traditional blacklists are populated with information from intelligence feeds, intrusion detection systems, honeypots, and log files. But we at Recorded Future posit that traditional blacklists can be bettered by incorporating threat intelligence from deep and dark Web sources.


By scouring the entire Web for mentions of known malware related to specific domains, we (https://www.recordedfuture.com/hunt/) were able to identify nearly 1,400 instances of malware-infested domains that were not recognized on established blacklists. Recorded Future analyzed 890,000 documents that mention malware (including Web pages, tweets, and pastes) from nearly 700,000 Web sources that we track with the Recorded Future Web index. This means that 92% of the suspicious IP addresses identified in our project were not found elsewhere on other blacklists!

It's important to note that in this particular test, the criteria for inclusion was two instances of malware mentions. When looking for suspicious domains with only one associated malware, the number of potential threats increases. Increasing the mentions of malware, we believe, increases the accuracy of the findings, meaning organizations can improve their threat intelligence (https://www.recordedfuture.com/cyber-threat-intelligence/) and threat detection capabilities, and drive down risks.



Network graph of 1,521 IP addresses (blue) and 198 malware (red).

To learn more about this threat intelligence research using hidden link analysis, please download the full report (<http://go.recordedfuture.com/two-shady-men-report>), “Two Shady Men Walk Into a Bar,” or contact us (<http://go.recordedfuture.com/cyber-demo>) for more information.



**TRENDING CYBER
VULNERABILITIES
DELIVERED TO
YOUR INBOX DAILY**

Sign up for the
Recorded Future Cyber Daily
and receive trending threat
insights every day by email.

- ✓ **Top Hackers**
- ✓ **Top Exploits**
- ✓ **Top Vulnerabilities**

SIGN UP

(http://go.recordedfuture.com/cs/c/?cta_guid=319b73dc-5d4b-4a28-9a22-951b4d3f1a24&placement_guid=34d9008b-bbf0-4c3f-9f9c-d335f0fc86b5&portal_id=252628&redirect_url=APefjpELTeON8r-5VTKj2B94wk81FpoTrkT3uywxgSzbwQ28h_GyQEKMOJOO2CVwaswhcludl9J50kXdvmnDSuRIZu9Dv538unhUF8rPW3Wum04z9q9m44qQWCmPrzG1f3Ch3cyT1mCnhMZjYj1UM8Qo4gBblnls3M&hsutkshady-men-report%2F&canon=https%3A%2F%2Fwww.recordedfuture.com%2Ftwo-shady-men-report%2F)

Related Articles

(<https://www.recordedfuture.com/cyber-threat-landscape-attackers/>)

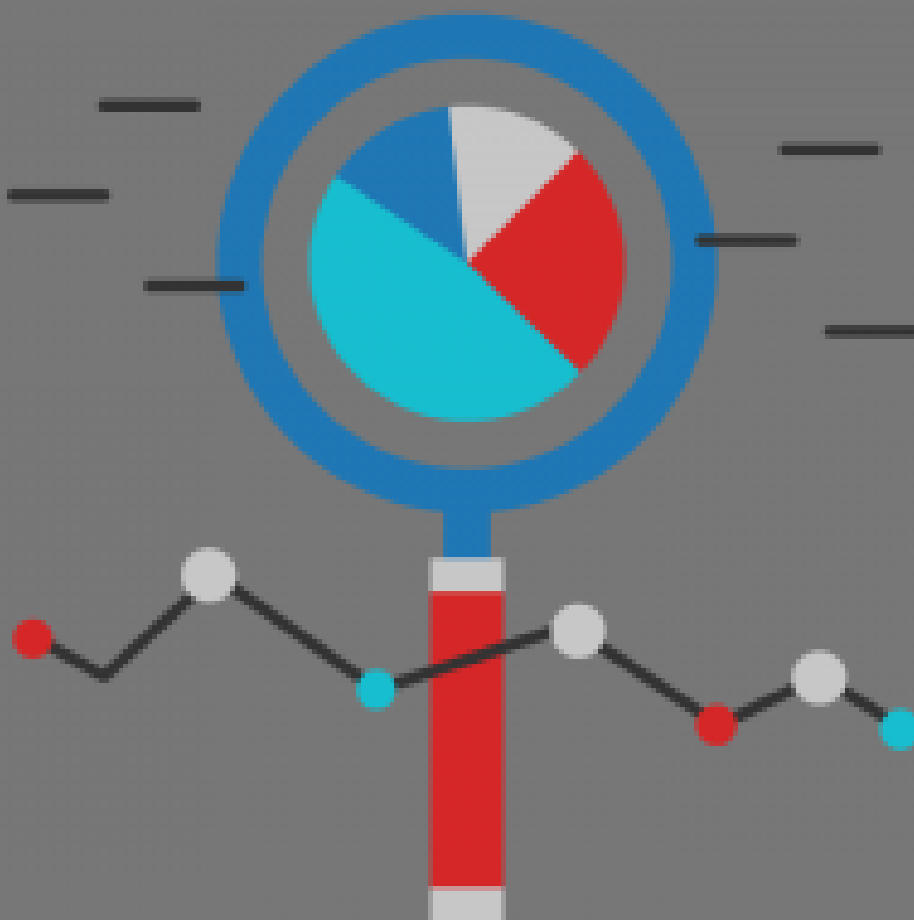


THE CONTEMPORARY CYBER THREAT LANDSCAPE

BLOG SERIES

Cyber Threat Landscape: Attackers and Operations (<https://www.recordedfuture.com/cyber-threat-landscape-attackers/>)

(<https://www.recordedfuture.com/attack-vector-trends/>)



Analyzing Attack Vector Trends by Industry, Country, and More (<https://www.recordedfuture.com/attack-vector-trends/>)

(<https://www.recordedfuture.com/week-to-week-report/>)



New Research Shows Most Vulnerabilities Exploited in About a Week
(<https://www.recordedfuture.com/week-to-week-report/>)

<https://www.recordedfuture.com/european-cyber-army-analysis/>



EUROPEAN CYBER ARMY

Why Security Teams Should Pay Attention to the European Cyber Army

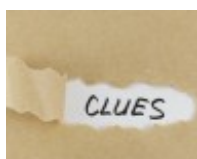
(<https://www.recordedfuture.com/european-cyber-army-analysis/>)



(<http://go.recordedfuture.com/cs/c/>)

cta_guid=49fb5194-0e1d-41bc-a25d-a060183c6ade&placement_guid=a3a005bc-e49a-43b1-a927-bb514f176b59&portal_id=252628&redirect_url=APefjpEncFVXrIBStdM1M8po5U2MiZnmNWPXNoZKKVjgMkaVxHx_xWqoB5FVYs7zP5_EF3m1rksTyHYFVJAZvDvL4jay86U17pCFV4UxZpTsk6QQK9Ishady-men-report%2F&canon=https%3A%2F%2Fwww.recordedfuture.com%2Ftwo-shady-men-report%2F)

Recent Blog Posts



MandaTORY Threat Intelligence: Clues From the Web (<https://www.recordedfuture.com/tor-threat-intelligence/>)

By Greg on September 3, 2015

(<https://www.recordedfuture.com/tor-threat-intelligence/>)



Get Schooled in Threat Intelligence: Cyber Daily Teaches the Biggest Threats

By Greg on September 1, 2015

(<https://www.recordedfuture.com/back-to-school/>)



OSINT for the Win! (HP) Protect Your Environment With Recorded Future ...

By Greg on August 27, 2015

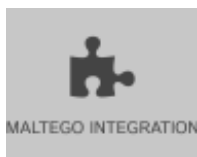
(<https://www.recordedfuture.com/hp-protect-2015/>)



Threat Intelligence Expert Perspective: Interview With Levi Gundert (<https://www.recordedfuture.com/levi-gundert-interview/>)

By Greg on August 26, 2015

(<https://www.recordedfuture.com/levi-gundert-interview/>)



Recorded Future Maltego Integration – Now With Moar (<https://www.recordedfuture.com/maltego-integration-improvements/>)

By Matt on August 17, 2015

(<https://www.recordedfuture.com/maltego-integration-improvements/>)



SUBSCRIBE TO OUR BLOG

Join over 14,000 intelligence analysts
and security professionals who
receive free Recorded Future content
as soon as it's published.

(<http://bit.ly/1pV4fIS>)



GET EMAIL UPDATES



(<http://feeds.feedblitz.com/recordedfuture>)



(<https://twitter.com/RecordedFuture>)



(<https://www.facebook.com/RecordedFuture>)



(<https://www.linkedin.com/company/recorded-future>)



(<http://www.youtube.com/user/RecordedFuture>)



(<https://plus.google.com/+recordedfuture>)

See Recorded Future's threat
intelligence in action.

REQUEST DEMO

RECENT BLOG POSTS ([HTTPS://WWW.RECORDEDFUTURE.COM/BLOG/](https://www.recordedfuture.com/blog/))

MandaTORy Threat Intelligence: Clues From the Web (<https://www.recordedfuture.com/tor-threat-intelligence/>)

Get Schooled in Threat Intelligence: Cyber Daily Teaches the Biggest Threats to Your Network (<https://www.recordedfuture.com/back-to-school/>)

OSINT for the Win! (HP) Protect Your Environment With Recorded Future and ArcSight (<https://www.recordedfuture.com/hp-protect-2015/>)

Threat Intelligence Expert Perspective: Interview With Levi Gundert (<https://www.recordedfuture.com/levi-gundert-interview/>)

@RECORDEDFUTURE ([HTTP://WWW.TWITTER.COM/RECORDEDFUTURE/](http://www.twitter.com/recordedfuture/))

RT @levigundert (<http://twitter.com/levigundert>): I heart #python (<http://twitter.com/search?q=%23python>) Unfortunately, so do those with malicious intent. @RecordedFuture (<http://twitter.com/RecordedFuture>) real-time #threatintelligence (<http://twitter.com/search?q=%23threatintelligence>) <http://t....> (<http://t....>)

The Cyber Daily is a real treat. It's like a #Snickers (<http://twitter.com/search?q=%23Snickers>) in your lunchbox! Learn more: <http://t.co/Suae6ApNa3> (<http://t.co/Suae6ApNa3>) #BackToSchool (<http://twitter.com/search?q=%23BackToSchool>)

Be there, or be vulnerable. Attend #RFUN15 (<http://twitter.com/search?q=%23RFUN15>) to learn about the latest in threat intelligence: <http://t.co/47fkebD5Si> (<http://t.co/47fkebD5Si>) #ThreatIntel (<http://twitter.com/search?q=%23ThreatIntel>) #InfoSec (<http://twitter.com/search?q=%23InfoSec>)

RECENT PRESS ([HTTPS://WWW.RECORDEDFUTURE.COM/PRESS/](https://www.recordedfuture.com/press/))

Blacklists Miss 90% of Malware Blogged IP Love

(http://www.theregister.co.uk/2015/08/12/two_shady_men_walk_into_a_bar_blacklist_report/)

New IP Address Blacklist Based on Web Chatter

(<http://www.csoonline.com/article/2969312/network-security/new-ip-address-blacklist-based-on-web-chatter.html>)

How to Surf the Dark Web for Fun and Profit

(<http://www.csoonline.com/article/2949304/cyber-attacks-espionage/how-to-surf-the-dark-web-for-fun-and-profit.html>)

Opinion: The Value of Unmasking Tor's Dark Side

(<http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0720/Opinion-The-value-of-unmasking-Tor-s-dark-side>)

COMPANY

About (<https://www.recordedfuture.com/about/>)

Contact (<https://www.recordedfuture.com/contact/>)

Press (<https://www.recordedfuture.com/press/>)

Events (<https://www.recordedfuture.com/events/>)

Services (<https://www.recordedfuture.com/services/>)

PRODUCTS

Cyber Threat Intelligence (<https://www.recordedfuture.com/cyber-threat-intelligence/>)

Corporate Security (<https://www.recordedfuture.com/corporate-security/>)

Competitive Intelligence (<https://www.recordedfuture.com/competitive-intelligence/>)

Defense Intelligence (<https://www.recordedfuture.com/defense-intelligence/>)

Web Intelligence Platform (<https://www.recordedfuture.com/web-intelligence/>)

CUSTOMERS

Login (<https://www.recordedfuture.com/live/login/>)

Support Center (<http://support.recordedfuture.com/>)

Software Status (<http://status.recordedfuture.com/>)

Source Suggestion (<https://www.recordedfuture.com/source-suggestion/>)

Developer Code (<https://code.google.com/p/recordedfuture/>)

Copyright © 2015 Recorded Future, Inc.

Privacy Policy (<https://www.recordedfuture.com/privacy-policy/>)

Terms of Use (<https://www.recordedfuture.com/terms-of-use/>)

API Terms of Use (<https://www.recordedfuture.com/api-terms-of-use/>)

Jobs (<https://www.recordedfuture.com/jobs/>)