Human Phishing Defense for the Enterprise

Stay ahead of emerging threats with IBM Security and Cofense

Cybercriminals are more sophisticated than ever, and the attacks on all types of organizations show no signs of slowing down. That's why IBM Security, Cofense and a wide range of security industry leaders have joined forces on the IBM Security App Exchange—so security teams from around the world can work together to create better network defenses.

Reduce phishing risk with Cofense Intelligence

Cofense Intelligence is 100% human-verified machine-readable threat intelligence (MRTI). Subscribers receive a fully-vetted source of intelligence into the App verified by Cofense researchers. Cofense also provides security teams with context around the criminal infrastructure to extend beyond a list of Indicators of Compromise (IOCs), and enable teams to see their adversary's full operation as opposed to one-offs that change rapidly. Customers enter Cofense-provided RESTful API credentials to ingest sources of phishing intelligence into the App and analysts can then operationalize their workflow based on phishing indicators.

Cofense Intelligence IOCs provide security teams with visibility into phishing criminal infrastructure. QRadar ingests and

IBM Security

The IBM Security App Exchange provides organizations with:

- Convenient web access to validated extensions to IBM Security solutions
- Additional IBM® Security QRadar® correlation rules, dashboards, visualizations and third-party integrations
- The ability to share content with industry peers to help eliminate threats

COFENSE

Cofense, Inc. 1602 Village Market Blvd, SE #400 Leesburg, VA 20175

PhishMe_Intelligence_Malware_URLs_Data (tables)

Outer Key	Provider	Impact Rating	First Seen Date	Last Seen Date	Identifier	Threat Details	Active Threat Report	Brand	Malware Family	Infrastructure
http://knuffieworld.de/index.png	PhishMe Intelligence	Major	1488388285112	1488388289250	8429.0	https://www.threathq.com/p42/search/default?m=8429	https://www.threathq.com/api/l/activethreatreport/8429/html	Generic Malware Threat	LNK downloader	Payload
http://groupcreatedt.at/x64.bin	PhishMe Intelligence	Major	1488388285112	1488388289250	8429.0	https://www.threathq.com/p42/search/default?m=8429	https://www.threathq.com/api/l/activethreatreport/8429/html	Generic Malware Threat	Ursnif	Payload
http://groupcreatedt.at/x32.bin	PhishMe Intelligence	Major	1488388285112	1488388289250	8429.0	https://www.threathq.com/p42/search/default?m=8429	https://www.threathq.com/api/l/activethreatreport/8429/html	Generic Malware Threat	Ursnif	Payload
http://fedisogfnes.com/0p8hcmk/index.php	PhishMe Intelligence	Major	1488380213390	1488380216366	8434.0	https://www.threathq.com/p42/search/default?m=8434	https://www.threathq.com/api/l/activethreatreport/8434/html	Generic Malware Threat	Nymaim	C2
https://wecrobat.co/faktor.exe	PhishMe Intelligence	Major	1488380213390	1488380216366	8434.0	https://www.threathq.com/p42/search/default?m=8434	https://www.threathq.com/api/l/activethreatreport/8434/html	Generic Malware Threat	OfficeMacro	Payload
http://eveningfloods.bid/counter/	PhishMe Intelligence	Major	1488383725157	1488402005287	8435.0	https://www.threathq.com/p42/search/default?m=8435	https://www.threathq.com/api/l/activethreatreport/8435/html	USPS	JSDropper	Payload
http://tuouyunittyewr.top/search.php	PhishMe Intelligence	Major	1488388146924	1488407549462	8437.0	https://www.threathq.com/p42/search/default?m=8437	https://www.threathq.com/api/l/activethreatreport/8437/html	Generic Malware Threat	OfficeMacro	Payload

provides analysts with intelligence to act based on phishing URLs, IPs, domains, files, command and control (C2), payload, and exfiltration sites. Indicators are supported by human-readable reports illustrating the phishing infrastructure with executive and technical reports. Security teams are much more confident in the action they take based on thorough indicator report analysis. Cofense Intelligence reports not only identify what is a security risk, but explicitly state why indicators are malicious so that analysts don't have to do additional research. Armed with human-verified intelligence indicators and verbose reports, security teams can defend the enterprise against the number one threat vector facing companies today – phishing.

Discover the IBM Security App Exchange

The IBM Security App Exchange is the premier collaboration site for sharing software enhancements, applications and extensions that complement IBM Security solutions. It enables security teams to access tools that help improve visibility into threats, anomalies and malicious activity occurring on the network, while also expanding the mitigation and remediation capabilities deeply integrated in the IBM QRadar Security Intelligence Platform.

For more information

To learn more about the IBM Security App Exchange, please visit: http://www-03.ibm.com/security/engage/app-exchange/

For more information about Cofense, please visit: www.cofense.com