侵入の痕跡（Indicators of Compromise, IoC）

SHA-256	ファイル名・概要	トレンドマイクロでの検出名
cfa3d506361920f9e1db9d8324dfbb3a9c79723e702d70c3dc8f51825c171420	ALL%20tim%20nha%20Chi%20Ngoc%20Canada.zip	Backdoor.MacOS.OCEANLOTUS.F
48e3609f543ea4a8de0c9375fa665ceb6d2dfc0085ee90fa22ffaced0c770c4f	ALL tim nha Chi Ngoc Canada	Backdoor.SH.OCEANLOTUS.F
05e5ba08be06f2d0e2da294de4c559ca33c4c28534919e5f2f6fc51aed4956e3	2nd stage fat binary	Backdoor.MacOS.OCEANLOTUS.F
fd7e51e3f3240b550f0405a67e98a97d86747a8a07218e8150d2c2946141f737	3rd stage fat binary	Backdoor.MacOS.OCEANLOTUS.F

ドメイン

- mihannevis[.]com
- mykessef[.]com
- idtpl[.]org

MITRE TTP

戦術	ID	名前	概要
Defense Evasion	T1070.004	File Deletion	アプリバンドルとドロッパーは実行後に自分自身を削除する
	T1222.002	Linux and Mac File and Directory Permissions Modification	バックドアは、実行するファイルのアクセス許可を+x に変更する
	T1027	Obfuscated Files or Information	読み取り可能な文字列は暗号化される
	T1036.005	Masquerading: Match Legitimate	アプリバンドルは、ユーザをだまして実行する文書ファイルになりすます

		Name or Location	
	T1070.006	Indicator Removal on Host: Timestomp	バックドアは、「touch」コマンドを利用して、作成されたファイルの日付と時刻を変更する
Discovery	T1082	System Information Discovery	バックドアは、C&C サーバに送信するさまざまな情報を収集する
Collection	T1560.003	Archive Collected Data: Archive via Custom Method	バックドアは、漏えいする前にデータを暗号化する
Command and Control	T1095	Non-Application Layer Protocol	前の検体と同様に、C&C データに基づいてバックドア動作を実行する

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com