侵入の痕跡（Indicators of Compromise，IoC）

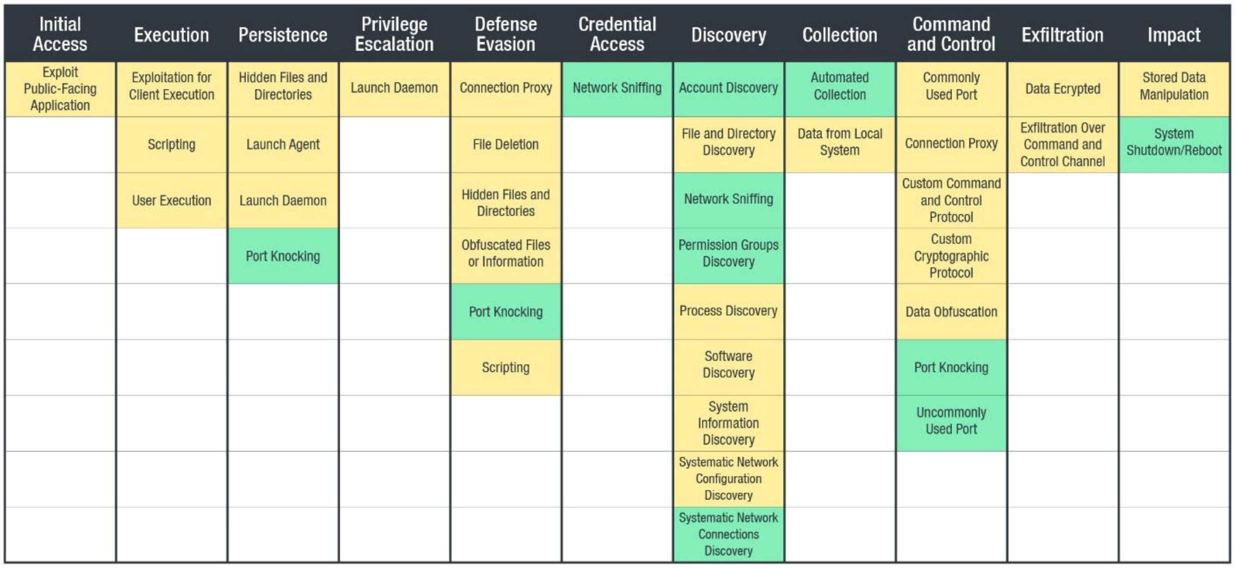
SHA256	ファイル名	検出名
846d8647d27a0d729df40b13a644f3bffdc95f6d0e600f2195c85628d59f1dc6	/Contents/Resources/Base.lproj/SubMenu.nib	Backdoor.MacOS.DACLS.A
d3235a29d254d0b73ff8b5445c962cd3b841f487469d60a02819c0eb347111dd	TinkaOTP.dmg	Backdoor.MacOS.DACLS.A
e5b842784cc3e9bc0376915d2d823c3e4e076d29b5fb98ea69ff9a56b0f4a54a		
216a83e54cac48a75b7e071d0262d98739c840fd8cd6d0b48a9c166b69acd57d		
7e8a086319a218732dde5a749afdd9813d3047eaeef511e0374ca64fd8d0d033		
899e66ede95686a06394f707dd09b7c29af68f95d22136f0a023bfd01390ad53		
fea0bd961d8d72642a3e1cb92b6ac084a9680eaef816ad414e282f6ea87d52c6	TinkaOTP.app	Backdoor.MacOS.DACLS.A
7b8792025aacff5dacb3a9121ec2f5bfa33d5932d1f43b9ad0d518c55c6e1298	/Contents/MacOS/TinkaOTP	Backdoor.MacOS.DACLS.A
90fbc26c65e4aa285a3f7ee6ff8a3a4318a8961ebca71d47f51ef0b4b7829fd0		

関連 URL

https[://]loneeaglerecords[.]com/wp-content/uploads/2020/01/images[.]tgz.001 Malware accomplice

MITRE ATT&CK Framework

解析中に確認された特徴を黄色でハイライト、C＆C サーバコマンドに基づく可能なアクションは緑でハイライトしています。



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application	Exploitation for Client Execution	Hidden Files and Directories	Launch Daemon	Connection Proxy	Network Sniffing	Account Discovery	Automated Collection	Commonly Used Port	Data Ecrypted	Stored Data Manipulation
	Scripting	Launch Agent		File Deletion		File and Directory Discovery	Data from Local System	Connection Proxy	Exfiltration Over Command and Control Channel	System Shutdown/Reboot
	User Execution	Launch Daemon		Hidden Files and Directories		Network Sniffing		Custom Command and Control Protocol		
		Port Knocking		Obfuscated Files or Information		Permission Groups Discovery		Custom Cryptographic Protocol		
				Port Knocking		Process Discovery		Data Obfuscation		
				Scripting		Software Discovery		Port Knocking		
						System Information Discovery		Uncommonly Used Port		
						Systematic Network Configuration Discovery				
						Systematic Network Connections Discovery				

-

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