日本の製造業を狙うTickグループ

macnica.net/mpressioncss/feature_05.html/

侵入拡大・目的実行

侵入後の攻撃者の内部活動の検出には、EDR製品が有効です。但し一般的なEDR群の製品が持つ脅威度の高い検知パターンとしては、MITER ATT&CK の攻撃の足場をつくる(Initial Access/Execution/Persistence/Privilege Escalation/Defense Evasion)フェーズが多く、攻撃者が足場づくりのフェーズを経て、遠隔操作で正規コマンドを使って内部での移動をし始めると、製品が持つ検知パターンでは攻撃の発見が難しくなる傾向があると思われます。特に標的型攻撃がEDR製品の導入前に始まっていたケースでは、足場をつくるフェーズが完了しているため、製品が持つ検知パターンでの検出漏れが懸念されます。EDR群の製品を導入した場合には、定期的に収集したログに含まれる正規コマンドの実行状況やそのコマンドがIT技術者以外の所有する端末によって頻繁に実行されていないかどうかといった視点で分析して、攻撃の検出漏れがないように注意して頂ければと思います。

Tactic	Technique	ID	備考
Initial Access	Exploit Public-Facing Application	T1190	国内資産管理ソフトの脆弱性を悪用
Spearphishing Attachment	T1193	なりすまし、侵害したメールアカウントから配送	
Supply Chain Compromise	T1195	海外拠点へ攻撃メールを配送	
Execution	Exploitation for Client Execution	T1203	Office製品脆弱性を悪用

Tactic	Technique	ID	備考
User Execution	T1204	アイコン偽装し、受信者に実行させる	
Command-Line Interface	T1059	ファイル削除のためにbatを起動	
Service Execution	T1035	サービスとして起動	
Rundll32	T1085	DLLの単独実行に使用	
Persistence	New Service	T1050	サービス登録
DLL Search Order Hijacking	T1038	正規ファイルが使うDLLと同じ名前にし、同一フォルダに設置	
Logon Scripts	T1037	ログオン時に自動実行されるようにレジストリを追加	
Registry Run Keys / Startup Folder	T1060	感染機器再起動後に自動実行されるようにレジストリ追加/スタートアップディレクトリにコピー	
Defense Evasion	Binary Padding	T1009	ドロップするファイルの肥大化
Deobfuscate/Decode Files or Information	T1140	検体内部の文字列を難読化して検出回避を試みる	
Code Signing	T1116	窃取した署名を付与	
Disabling Security Tools	T1089	アンチウイルス製品を停止	
Software Packing	T1045	商用パッカーなどを利用	
Process Hollowing	T1093	svchost.exeを起動、インジェクション	
File Deletion	T1107	使い終わったファイルを削除	
Hidden Files and Directories	T1158	ドロップするファイルに隠し属性設定	
DLL Side-Loading	T1073	DLL(マルウェア)をロードする正規EXEを合わせて設置	
Credential Access	Credential Dumping	T1003	Mimikatzを使用

Tactic	Technique	ID	備考
Discovery	System Information Discovery	T1082	dirコマンドでファイル探索
Account Discovery	T1087	net user コマンドでユーザを探索	
Network Share Discovery	T1135	net share, net view コマンドで探索	
System Network Connection Discovery	T1049	netstat コマンドでリモートデスクトップ等を探索	
Process Discovery	T1057	tasklist コマンドで探索	
Lateral Movement	Windows Admin Shares	T1077	感染拡大にPsExecを使用
Remote File Copy	T1105	Datper等のRATを使い、感染機器へファイルアップロード/ダウンロードを行う	
Collection	Data from Local System	T1005	cmdを使い感染機器の情報を収集
Command And Control	Commonly Used Port	T1043	80, 443を使用
Custom Cryptographic Protocol	T1024	AES, RC4, XOR等を使い暗号化	
Data Encoding	T1132	base64を使い通信をエンコード	
Data Obfuscation	T1001	マルウェアが埋め込まれた画像ファイルをダウンロード	
Standard Application Layer Protocol	T1071	HTTP, HTTPSでC&Cサーバと通信	
Standard Cryptographic Protocol	T1032	RC4, AESでHTTP送信データを暗号化	
Web Service	T1102	正規サイトを改ざんし、C&Cサーバとして使用	
Exfiltration	Exfiltration Over Command and Control Channel	T1041	RATを使い、C&Cサーバへファイルをアップロード

Tactic	Technique	ID	備考
Data Compressed	T1002	zip, makecabコマンドでファイルを圧縮	

表2 MITRE ATT&CK Technique

赤字のテクニックは、弊社で多く観測し確認を重視した方が良いと考えているものです。

以下Tickに関連するインディケータは、大半が過去弊社レポートに含まれているものですが、インシデント調査、対応にてご活用頂ければと考え改めて記載します。

インディケータ	タイプ	備考
a04d2668b1853051dd5db78721b7deae7490dbd60cef96d55cc91ff8c5d4730d	SHA256	XXMM
d91894e366bb1a8362f62c243b8d6e4055a465a7f59327089fa041fe8e65ce30	SHA256	Datper
706a6833b4204a89455f14387dbfc4903d18134c4e37c184644df48009bc5419	SHA256	Datper
fdd4a4b3d56217579f4cd11df65cf4bd4c60cac428aa649d93227604fbb8b49e	SHA256	Exploit ppsx
569ceec6ff588ef343d6cb667acf0379b8bc2d510eda11416a9d3589ff184189	SHA256	Datper
e38d3a7a86a72517b6ebea89cfd312db0f433385a33d87f2ec8bf83a62396bb3	SHA256	Datper
6530f94ac6d5b7b1da6b881aeb5df078fcc3ebffd3e2ba37585a37b881cde7d3	SHA256	Datper
569ceec6ff588ef343d6cb667acf0379b8bc2d510eda11416a9d3589ff184189	SHA256	Datper
0542ecabb7654c6fd6fc4e12fe7f5ff266df153746492462f7832728d92a5890	SHA256	RAT Loader
d705734d64b5e8d61687db797d7ad3211e99e4160c30ba209931188f15ced451	SHA256	RAT Loader
3f5a5819d3fe0860e688a08c1ad1af7208fe73fd9b577a7f16bcebf2426fbdaf	SHA256	RAT Loader
911fbd95e39db95dbfa36ff05d7f55fc84686bbe05373fc2f351eb76a15d9d74	SHA256	Downloader
337d610ebcc9c0834124f3215e0fe3da6d7efe5b14fa4d829d5fc698deca227d	SHA256	Downloader
706a6833b4204a89455f14387dbfc4903d18134c4e37c184644df48009bc5419	SHA256	Downloader
58b06982c19f595e51f0dc5531f6d60e6b55f775fa0e1b12ffd89d71ce896688	SHA256	Downloader
1fdd9bd494776e72837b76da13021ad4c1b3a47c8a49ca06b41dab0982a47c7e	SHA256	Dropped Word Plugin DLL
fb0d86dd4ed621b67dced1665b5db576247a10d43b40752c1236be783ac11049	SHA256	Downloader
d1307937bd2397d92bb200b29eeaace562b10474ff19f0013335e37a80265be6	SHA256	Downloader
32dbfc069a6871b2f6cc54484c86b21e2f13956e3666d08077afa97d410185d2	SHA256	Downloader
80ffaea12a5ffb502d6ce110e251024e7ac517025bf95daa49e6ea6ddd0c7d5b	SHA256	down_new

インディケータ	タイプ	備考
ec052815b350fc5b5a3873add2b1e14e2c153cd78a4f3cc16d52075db3f47f49	SHA256	version RAT
http://www[.]cheapraybanoutletonline[.]com/fooler.php	C2	XXMM
http://www[.]<redacted>[.]co[.]jp/halftime/other/goods.php	C2	Datper
www[.]aromatictree[.]co[.]kr	C2	Datper
http://211.233.81[.]242/hp.php	C2	Datper
robot[.]softsrobot[.]com:443	C2	RAT Loader
www[.]runinngboys[.]com:443	C2	RAT Loader
dns[.]safedexperiences[.]com	C2	RAT Loader
google[.]safedexperiences[.]com	C2	RAT Loader
web[.]birthhappiness[.]com	C2	RAT Loader
www[.]birthhappiness[.]com	C2	RAT Loader
www[.]efficitivesubject[.]com	C2	RAT Loader
www[.]korlearn[.]com	C2	RAT Loader
www[.]miniiants[.]com	C2	RAT Loader
www[.]safedexperiences[.]com	C2	RAT Loader
dndns8866[.]com	C2	RAT Loader
efficitivesubjectapp[.]com	C2	RAT Loader
korlearn2030[.]com	C2	RAT Loader
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1)	User-Agent	XXMM
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	User-Agent	Datper
d4fy3ykdk2ddssr	Mutex	Datper

表3 痕跡情報（IOC）

他攻撃者グループBlackTechやEmdivi のTTPは下記レポートに記載してありますので、ご参照下さい。