

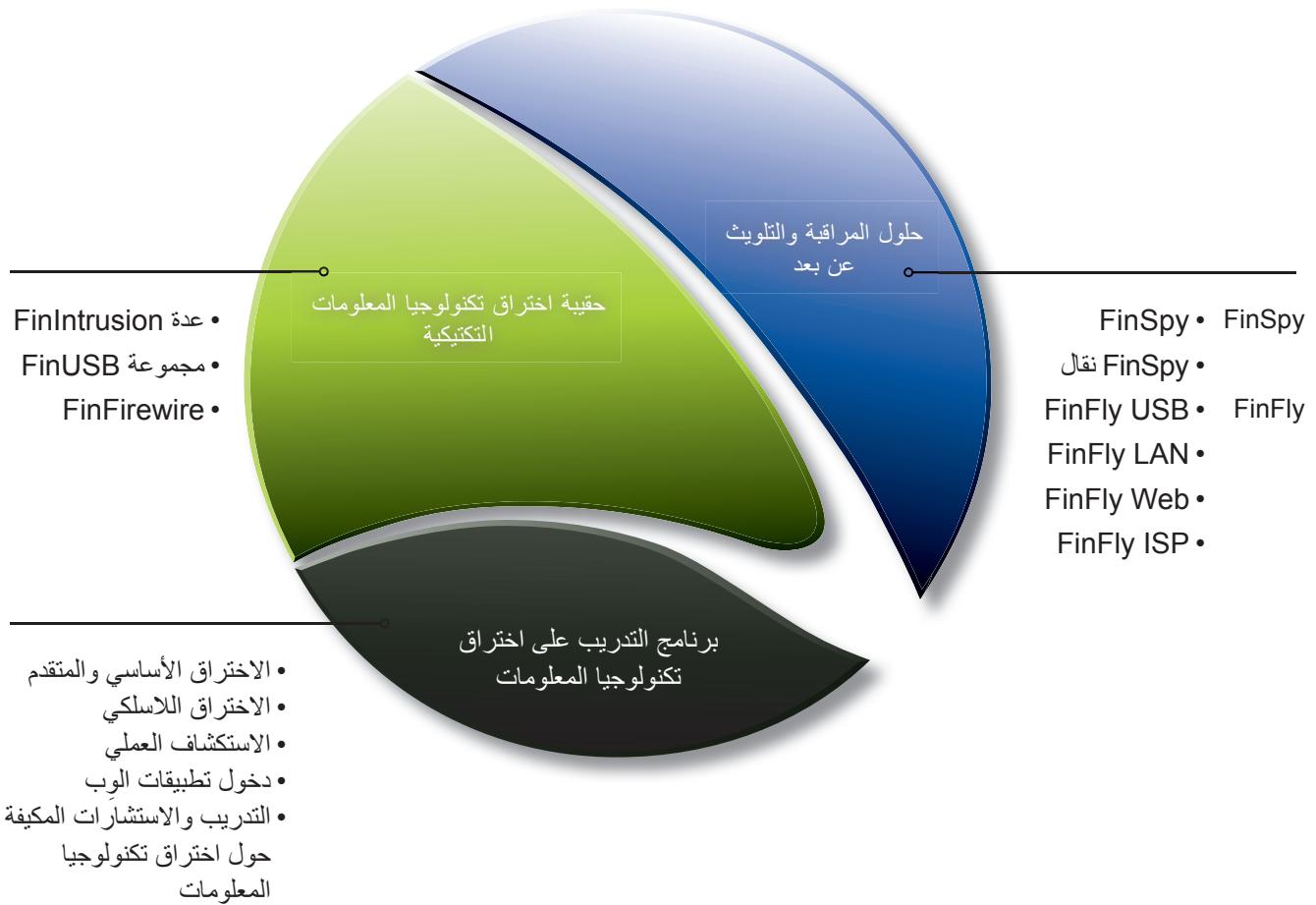


FINFISHER: حلول اختراق تكنولوجيا المعلومات
والمراقبة عن بعد للحكومات



FINFISHER™
IT INTRUSION

WWW.GAMMAGROUP.COM



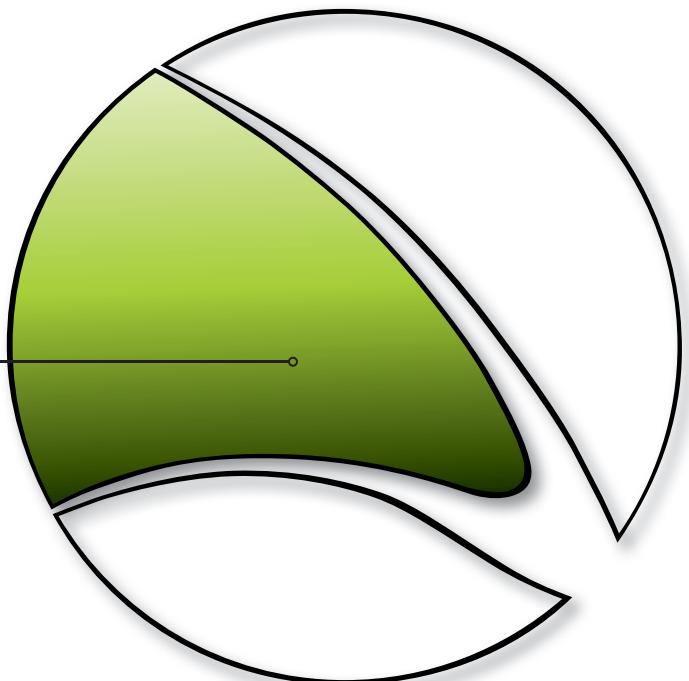
حقيبة اختراق تكنولوجيا المعلومات التكتيكية

FININTRUSION عدّة

FINUSB مجموعة

FINFIREWIRE

تعنى Gamma بالتطورات في مجال اختراق تكنولوجيا المعلومات بواسطة حلول تعزز قدرات عملائنا. تكمل حلول وتقنيات حديثة وسهلة الاستخدام دراية الوكالات الاستخباراتية وتمكنها من معالجة تحديات الاختراق التكتيكيًّا.



FINFISHER™
IT INTRUSION

WWW.GAMMAGROUP.COM

حقيقة اختراق تكنولوجيا المعلومات التكتيكية

عدة FININTRUSION

معلومات سريعة	
عمليات تكتيكية	الاستخدام:
عمليات استراتيجية	
كسر تشغيل WEP/WPA مراقبة الشبكات (بما في ذلك التشفير بواسطة نظام أمن الاتصالات) هجمات اختراق تكنولوجيا المعلومات	القدرات:
برمجيات وتجهيزات	المحتوى:

مثال الاستخدام ٢ : أمن تكنولوجيا المعلومات
استخدم علماً كثيرون عدة FinIntrusion لتقليد أمن بعض الشبكات وأنظمة الكمبيوتر لغایات هجومية ودفاعية باستخدام أدوات وتقنيات مختلفة.

مثال الاستخدام ٣ : برمجيات استراتيجية لتقديم استجابة الأنظمة
تستخدم عدة FinIntrusion للولوج عن بعد إلى حسابات بريد المستهدفين وإلى خوادم الويب الخاصة بهم (المدونات ومنتديات المناقشة) ولمراقبة نشاطاتهم وسجلات لوจهم وغيرها.

عدة FinIntrusion هي نتاج عمل متخصصين عالميين في مجال اختراق تكنولوجيا المعلومات، يتمتعون بما يزيد عن عشر سنوات من الخبرة في مجالهم بعد عملهم في فرق أمنية في القطاعين الخاص والعام وتجربتهم الطويلة في تقديم مستوى سلامـة وأمن شبـكات ومنظـمات متـعدـدة.

عدة FinIntrusion هي عدة تشغيلية حديثة وسرية يمكن استخدامها في غالبية عمليات اختراق تكنولوجيا المعلومات أكانت دفاعية أو هجومية. ومن بين عملائنا الحاليين الأقسام العسكرية التي تعنى بحرب الإنترنت والوكالات الاستخباراتية واستخبارات الشرطة ووكالات أخرى موكلة تطبيق القانون.

مثال الاستخدام ١ : وحدة المراقبة التقنية

استخدمت عدة FinIntrusion لفك تشفير بروتوكول الوصول الآمن للشبكة اللاسلكية (WPA) لشبكة مستهدفة لاسلكية منزلية، ومن ثم لمراقبة بريده الإلكتروني على الويب (Yahoo وGmail...) وشبكاته الاجتماعية (Facebook وMySpace...)... وقد مكن ذلك المحققين من مراقبة هذه الحسابات عن بعد انطلاقاً من مقراتهم من دون أن يحتاجوا إلى الاقتراب في مستهدفـهم.

لمحة شاملة على المميزات

- تكشف الشبكات اللاسلكية (٨٠٢,١١) وأجهزة البلوتوث
- تستعيد الخصوصية المكافحة للشبكات السلكية (WEP) (٦٤ و ١٢٨ بت) وعبارات المرور في غضون ٢ إلى ٥ دقائق
- تكسر عبارات مرور WPA ١ و WPA ٢ بواسطة «هجمات القاموس» (Dictionary Attacks)
- تراقب بشكل ناشط الشبكات المحلية (السلكية واللاسلكية) وتستخرج أسماء المستخدمين وكلمات المرور حتى بالنسبة إلى الجلسات المشفرة نظام أمن الاتصالات/طقة النقل الآمن
- تقلد نقطة الوصول اللاسلكي (٨٠٢,١١)
- تدخل عن بعد إلى حسابات البريد الإلكتروني باستخدام تقنيات اختراق تعتمد على الشبكات أو الأنظمة أو كلمات المرور
- تقييم أمن الشبكة والتأكد عليه

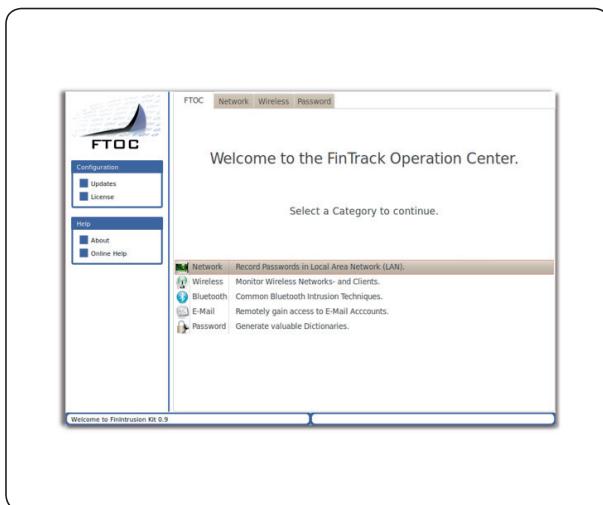
للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حقيقة اختراق تكنولوجيا المعلومات التكتيكية

عدة FININTRUSION

عناصر المنتج



مركز عمليات FinTrack

- واجهة بينية لهجمات اختراق تكنولوجيا المعلومات المؤتمتة

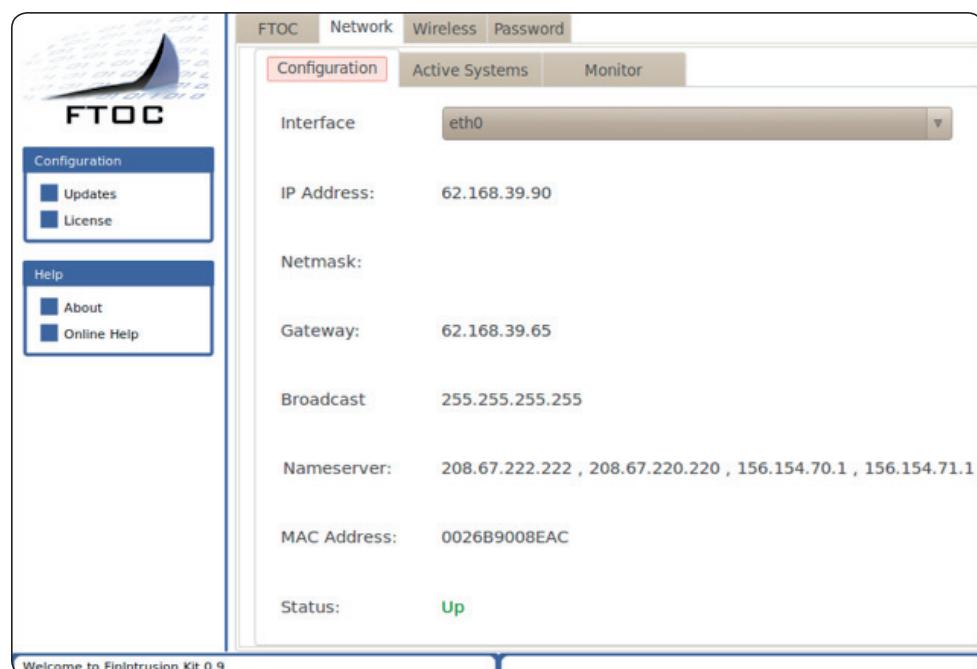


عدة تكتيكية سرية -FinIntrusion

العناصر الأساسية لاختراق تكنولوجيا المعلومات:

- مهابي WLAN بطاقة عالية
- مهابي بلوتوث بطاقة عالية
- هوانيات ٨٠٢,١١
- والكثير من الأدوات الأخرى لاختراق تكنولوجيا المعلومات

مراقبة الشبكات المحلية والشبكات اللاسلكية المؤتمتة



حقيقة اختراق تكنولوجيا المعلومات التكتيكية

عدة FININTRUSION

برنامج الكشف عن كلمات السر في الشبكات المحلية والشبكات اللاسلكية

- يكشف عن البيانات المشفرة بنظام أمن الاتصالات كالبريد الإلكتروني على الويب وبوابات الفيديو والصيরفة عبر الإنترنت،
الخ...

Main	Credentials		
Username	Password	Server	Protocol
dropbox	fr33dom	64.223.183.17	https
ftp	secret1	128.101.240.212	ftp
ftoc	password1	62.84.74.92	pop3

Start Delete Save...



حقيقة اختراق تكنولوجيا المعلومات التكتيكية

مجموعة FINUSB

معلومات سريعة	
عمليات تكتيكية	الاستخدام:
جمع المعلومات الولوج إلى النظام الحصول على معلومات جنائية سريعة	القدرات:
برمجيات	المحتوى:

مثال الاستخدام ٢ : وحدة المراقبة التقنية

كانت إحدى وحدات المراقبة التقنية تتبع مستهدفةً كان يزور مقاهي إنترنت مختلفة بشكل عشوائي ما جعل من المستحيل مراقبته بواسطة تقنية شبيهة بمحصص طروادة. استخدم FinUSB لاستخراج البيانات المتبقية على المنافذ العامة التي استخدمها المستهدف بعد مغادرته. يمكن أن تتم استعادة مستندات كثيرة فتحها المستهدف على بريده الإلكتروني بهذه الطريقة. وضمت المعلومات المجمعة بشكل أساسي ملفات Office أساسية وتاريخ التصفح من خلال تحليл سجلات المتصفحات وأكثر.

مجموعة FinUSB هي عبارة عن منتج من مهندس الوكلاء الموكلة تطبيق القانون والوكالات الاستخباراتية من استخراج المعلومات الجنائية بطريقة سريعة وآمنة من أنظمة الكمبيوتر دون اللجوء إلى عملاء متخصصين في تكنولوجيا المعلومات.

لقد تم استخدام هذه المجموعة بنجاح في عمليات حول العالم في أماكن تم العثور فيها على معلومات استخباراتية قيمة حول مستهدفين، في عمليات سرية ومكشوفة.

مثال الاستخدام ١ : عملية سرية

أعطي مخبر في إحدى منظمات الجريمة المنظمة جهاز FinUSB لتوثيق البرمجيات. استخرج بسرية تامة، معلومات خاصة بحسابات الويب والبريد الإلكتروني ومستندات Microsoft Office من الأنظمة المستهدفة بينما استخدمت المنظمة جهاز USB لتتبادل الملفات العادية كالموسيقى وأفلام الفيديو وملفات Office.

بعد إعادة جهاز USB إلى المقر، أتيح فك شفرة البيانات المجمعة وتحليلها واستخدامها لمراقبة المجموعة عن بعد بشكل مستمر.

لمحة شاملة على المميزات

- مستمثلاً للعمليات السرية
- سهولة الاستخدام من خلال التنفيذ الآلي
- ضمان التشفير بواسطة خوارزمية RSA وعيار التشفير المتتطور AES
- استخراج أسماء المستخدمين وكلمات المرور الخاصة بهم للبرمجيات الشائعة مثل:
 - برامج عمليل البريد الإلكتروني
 - برامج التراسل الفوري
 - المتصفحات
 - أدوات الإدارة عن بعد
- النسخ الصامت للملفات (البحث في القرص الصلب، وسلة المهامات والملفات التي فتحت أو صحيحة أو أنشئت مؤخرًا)
- استخراج معلومات خاصة بالشبكة (سجلات المحادثات وتاريخ التصفح ومفاتيح WEP/WEP(٢)(٢)...)
- مراقبة معلومات النظام (البرمجيات العاملة/المركبة، معلومات القرص الصلب، ...)

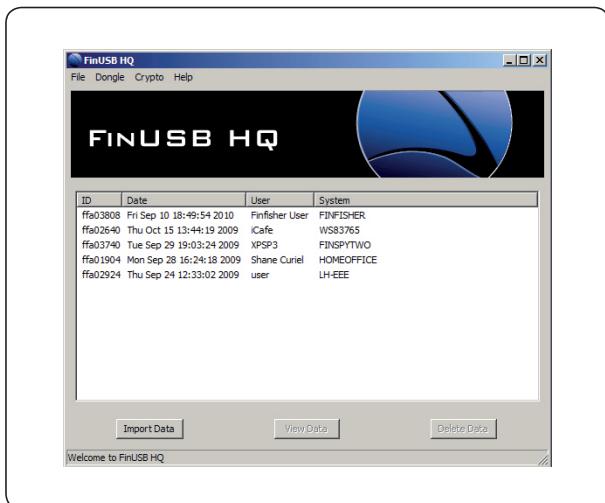
للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حقيقة اختراق تكنولوجيا المعلومات التكتيكية

مجموعة FINUSB

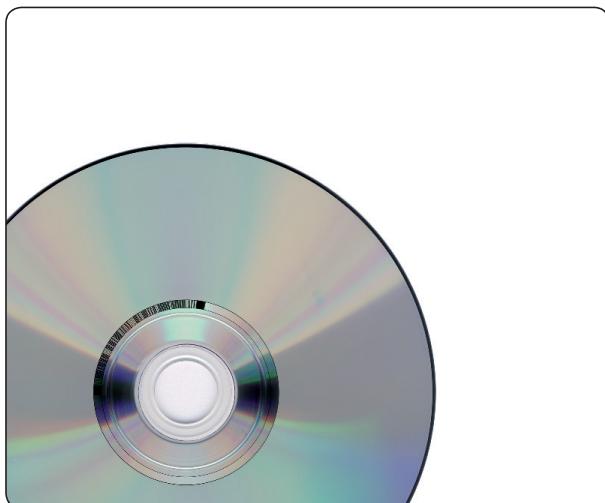
عناصر المنتج



FinUSB HQ

- واجهة مستخدم ببنية لفك شفرة البيانات المجمعة وتحليلها
- تشكيل الخيارات التشغيلية لجهاز توسيق البرمجيات

مجموعة FINUSB - وحدة نقالة



Windows - تجاوز حماية كلمات المرور في FinUSB

- تجاوز تسجيل الدخول إلى Windows من دون تغييرات دائمة في النظام

١٠ أجهزة لتوسيق البرمجيات (U3 - ١٦ جيجابايت)

- يستخرج بسرية البيانات
- يشفر البيانات فوراً

حقيقة اختراق تكنولوجيا المعلومات التكتيكية

مجموعة FINUSB

سهولة الاستخدام

١. اختر جهاز FinUSB لتوثيق البرمجيات



٢. قم بتشكيل المميزات/الزجل كلها التي ترغب فيها وحدث جهاز FinUSB HQ لتوثيق البرمجيات خاصتك بواسطة



٣. توجه إلى نظامك المستهدف



٤. قم بوصول جهاز توثيق البرمجيات Fin USB إليه



٥. انتظر حتى يتم نقل البيانات كلها



٦. عد إلى FinUSB HQ



٧. استورد البيانات كلها من جهاز توثيق البرمجيات FinUSB



٨. أعط التقرير



تقارير احترافية



حقيقة اختراق تكنولوجيا المعلومات التكتيكية

FINFIREWIRE

معلومات سريعة	
عمليات تكتيكية	الاستخدام:
تجاوز كلمة مرور المستخدم الولوج السري إلى النظام إتاحة التحقيق المباشر	القدرات:
برمجيات وتجهيزات	المحتوى:

مثال الاستخدام ٢ : استعادة كلمة السر

إن استعمال المنتج مع تطبيقات جنائية تقليدية مثل® Encase استخدمت الوحدات الجنائية وظيفية تفريغ الذاكرة العشوائية للحصول على لمحه عن معلومات الذاكرة العشوائية المتوفرة كما استعادوا كلمة السر المشفرة للقرص الصلب التي تم وضعها بواسطة برمجيات TrueCrypt التي شفرت القرص الصلب كاملاً.

يواجه كل من وحدات المراقبة والخرباء الجنائيون وضعًا يحتاج فيه إلى ولوج نظام كمبيوتر عامل من دون إطافاته تقليدياً لفقدان البيانات أو توفيرًا منهم لوقت في خلال عملية. في معظم الحالات، تتم حماية النظام المستهدف بواسطة حافظ شاشة مغلق بكلمة مرور أو لا يكون المستخدم قد كتب كلمة السر ليج إلى النظام بينما تكون شاشة الدخول عاملة. يمكن FinFireWire المشغل من تجاوز الشاشة المغلقة بكلمة مرور بسرعة وسريعة تامة والولوج إلى النظام المستهدف من دون ترك أي أثر أو تشويه أي إثبات جنائي

مثال الاستخدام ١ : العمليات الجنائية

دخلت إحدى الوحدات الجنائية منزل أحد المستهدفين وحاولت الولوج إلى نظام جهاز الكمبيوتر خاصته. كان الجهاز عاملًا، غير أن الشاشة كانت مغلقة.

ونظرًا إلى أن الوحدة لم تكن مخولة استخدام حل مراقبة عن بعد لأسباب قانونية، كانت لتفقد البيانات كلها باطفاء النظام بما أن القرص الصلب كان مشفرًا. تم استخدام FinFireWire لفتح قفل النظام المستهدف العامل ما مكّن العميل من نسخ الملفات كلها قبل إطفاء جهاز الكمبيوتر وأخذه إلى المقر.

لمحة شاملة على المميزات

- يحل أفال كل من حسابات المستخدم
- يفتح حافظ الشاشة المحمي بكلمة مرور
- يفرغ الذاكرة العشوائية للتحليل الجنائي
- يتيح القيام بالتحقيق المباشر من دون الحاجة إلى إعادة تشغيل النظام المستهدف
- لا يتم تغيير كلمة مرور المستخدم
- يعمل على Linux و Mac و Windows و FireWire و PCMCIA و 1394 و Express Card
- يعمل مع IT INTRUSION

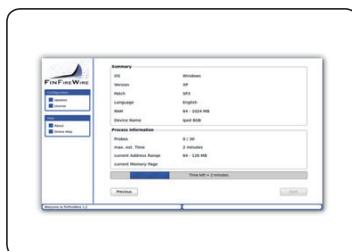
للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حقيقة اختراق تكنولوجيا المعلومات التكتيكية

FINFIREWIRE

عناصر المنتج



- واجهة مستخدم ببنية أشر وانقر
- واجهة مستخدم ببنية سهلة الاستخدام



- وحدة التكتيكية FinFireWire
- نظام تكتيكي كامل



مجموعة Universal FinWire كابلات

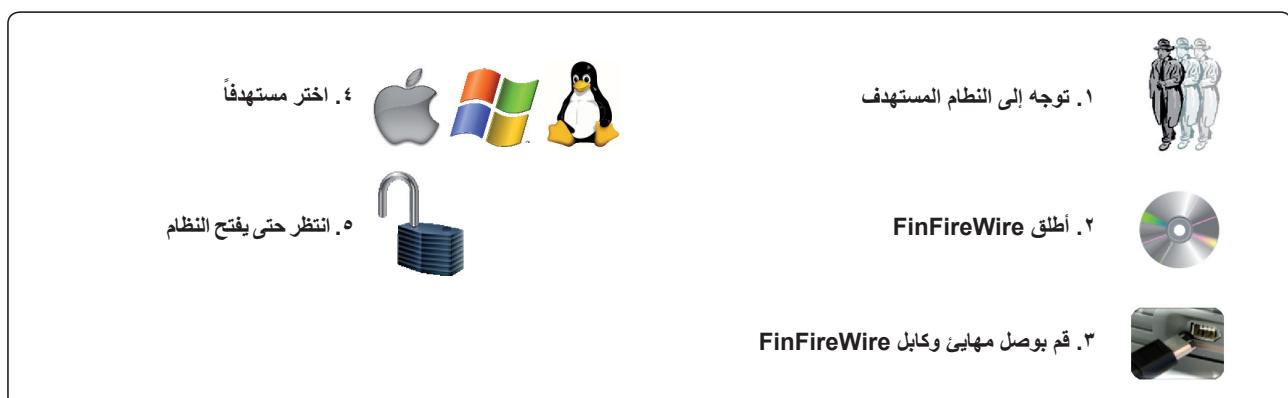
- pin 40 إلى pin 4
- pin 40 إلى pin 6
- pin 6 إلى pin 60



بطاقات توسيعة الشبكة

- بطاقات ExpressCard و بطاقات PCMCIA
- للانظمة المستهدفة غير المزودة بمنفذ FireWire

الاستخدام



GAMMA INTERNATIONAL
المملكة المتحدة



هاتف: +44 111 332 411 - 1264
فاكس: +44 111 332 422 - 1264

info@gammagroup.com

المعلومات التي يحويها هذا المستند سرية وهي عرضة للتغيير من دون إشعار مسبق. Gamma Group International غير مسؤولة عن الأخطاء التقنية أو التحريرية ولا عن أي معلومات محفوظة من هذا المستند.

حلول المراقبة والتلویث عن بعد

FINSPY

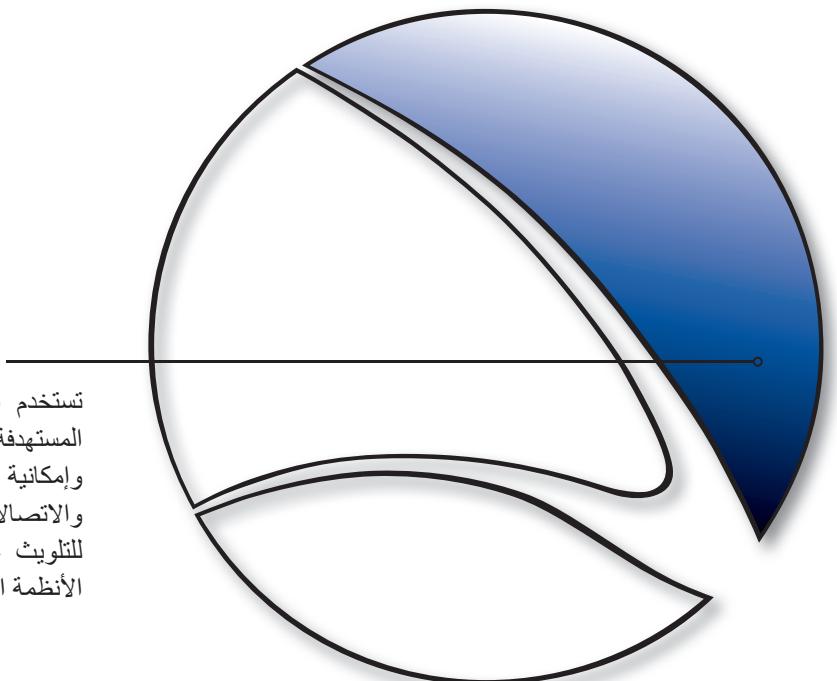
FINSPY MOBILE

FINFLY USB

FINFLY LAN

FINFLY WEB

FINFLY ISP



تستخدم المراقبة عن بعد و حلول التلویث للنفاذ إلى البرامج المستهدفة و هما يتيحان الولوج التام إلى المعلومات المخزنة و إمكانية التحكم بوظائف الأنظمة المستهدفة إلى حد التقاط البيانات والاتصالات المشفرة. إذا استعملت هذه الحلول مع طرق معززة للتلویث عن بعد، ستتيح لوكالات الحكومة القدرة على تلویث الأنظمة المستهدفة عن بعد.



FINFISHER™
IT INTRUSION

WWW.GAMMAGROUP.COM

حلول المراقبة والتلویث عن بعد

FINSPY

معلومات سريعة

عمليات استراتيجية	الاستخدام:
عمليات تكتيكية	
مراقبة الكمبيوتر عن بعد	القدرات:
مراقبة الهاتف النقالة عن بعد	
برمجيات	المحتوى:

مثال الاستخدام ٢ : الجريمة المنظمة

تم نشر FinSpy سرًا فيفي أنظمة مستهدفة تعود لأفراد إحدى مجموعات الجرائم المنظمة. ومن خلال التعقب والنفاذ عن بعد إلى المحادثات التي تتم عبر الميكروفونات فتم تجميع المعلومات الأساسية كلها من الاجتماعات كلها التي أقامتها تلك المجموعة.

FinSpy هو حل للمراقبة عن بعد أثبتت فعاليته على الأرض وهو يمكن الحكومات من مواجهة التحديات الراهنة في ما يتعلق بمراقبة المستهدفين المتنقلين والذين يتمتعون بالوعي الأمنية ويغيرون مواقعهم باستمرار ويستعملون قنوات تواصل مشفرة ومجهولة و/ أو يقيمون في الخارج.

حلول الاعتراف القانوني التقليدية تواجه تحديات جديدة يمكن حلها بشكل استثنائي من خلال أنظمة ناشطة مثل FinSpy:

- بيانات لا تنتقل عبر أي شبكة
- عمليات تواصل مشفرة
- مستهدفون متواجدون في الخارج

تم إثبات نجاح FinSpy لسنوات طويلة في عمليات حول العالم وجمعت بواسطته معلومات استخباراتية قيمة حول أفراد أو منظمات مستهدفة. عندما يتم تركيب FinSpy على نظام كمبيوتر، يمكن التحكم به عن بعد وولوجه فور وصله إلى الإنترنت/الشبكة، أيًّا كان النظام المستهدف في العالم.

مثال الاستخدام ١ : وكالة استخباراتية

تم تنزيل FinSpy على أنظمة كمبيوتر متعددة داخل مقاهي الإنترنت والأماكن الخطيرة لمراقبتها والكشف عن الأعمال المشبوهة فيها، خصوصاً التواصل عبر Skype مع الأفراد في الخارج. باستخدام الكاميرا، تم التقاط صور للمستهدفين بينما كانوا يستخدمون النظام.

لمحة شاملة على الميزات

الكمبيوتر المستهدف - أمثلة عن الميزات:

- حماية الإثباتات (إثباتات صالحة وفقاً للمعايير الأوروبية)
- إدارة المستخدمين وفقاً لتصاريح الأمان
- تشفير البيانات الأمنية وتنافقها بواسطة RSA ٤٠٨ و AES ٢٥٦

- يمنأ عن العامة من خلال برامج إخفاء الهوية
- يمكن إدماجه بسهولة بوظيفة LEMF

للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.

- تجاوز ٤٠ نظاماً مختبراً مضاداً للفيروسات
- تواصل سري مع المقر
- مراقبة Skype بالكامل (الاتصالات والدردشة ونقل البيانات والفيديو ولائحة الأسماء)
- مراقبة مباشرة عبر كاميرا الويب والميكروفون
- تسجيل التواصل العادي كالبريد الإلكتروني وجلسات الدردشة والصوت عبر بروتوكول الإنترنت
- تعقب المستهدف عبر البلدان
- استخراج «صامت» للملفات من القرص الصلب
- راصد لوحة مفاتيح قائم على نوع العملية لتحليل أسرع
- تحليل جنائي مباشر للنظام المستهدف
- مرشحات متقدمة لتسجيل المعلومات المهمة دون سواها (Mac OSX و Windows)
- يعمل مع غالبية أنظمة التشغيل (Mac OSX و Windows)



حول المراقبة والتلویث عن بعد

FINSPY

عناصر المنتج



FinSpy Agent

- ## •واجهة رسومية للجلسات المباشرة والتشكيل وتحليل البيانات الخاصة بالمستهدفين

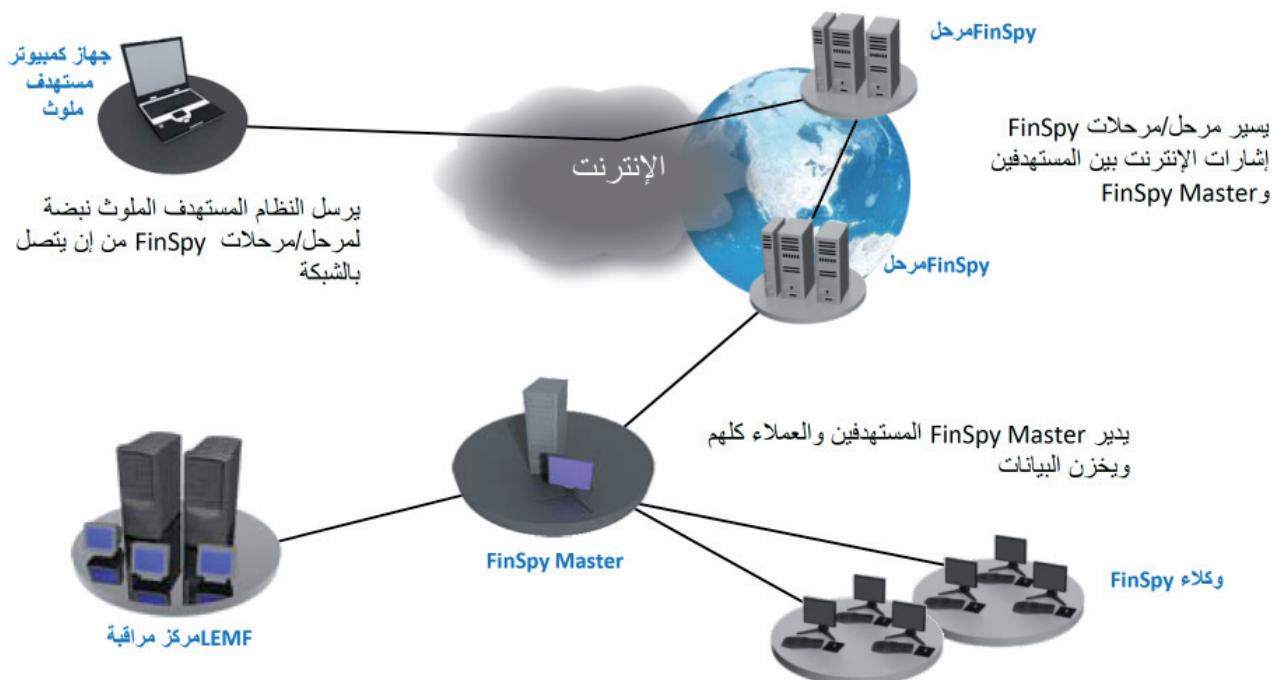
نیابی FinSpy Master و نظام

- تحكم كامل بالأنظمة المستهدفة
 - حماية الإثباتات لسجلات البيانات والنشاطات
 - تخزين آمن
 - إدارة المستخدمين والمستهدفين القائمة على تصاريح الأمان

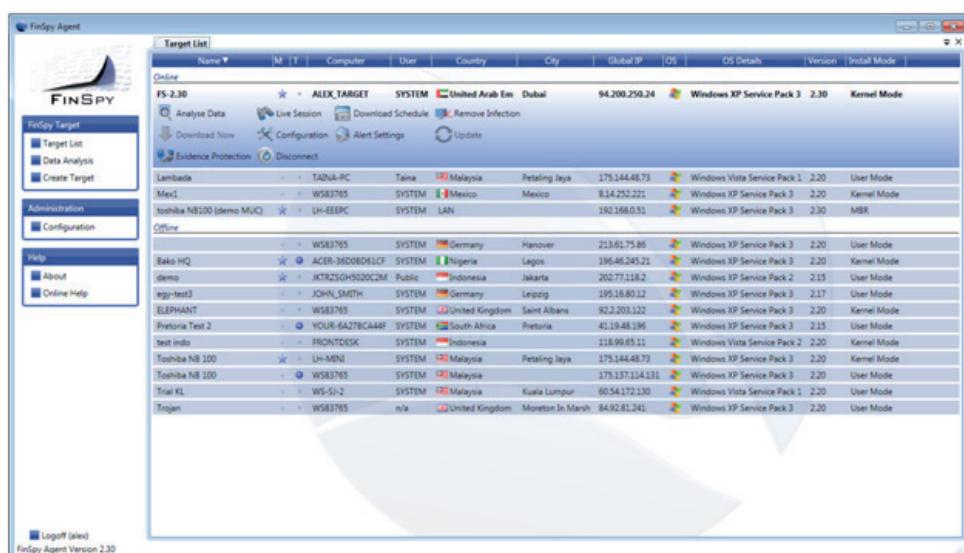
حلول المراقبة والتلویث عن بعد

FINSPY

الولوج إلى أنظمة كمبيوتر المستهدفين حول العالم



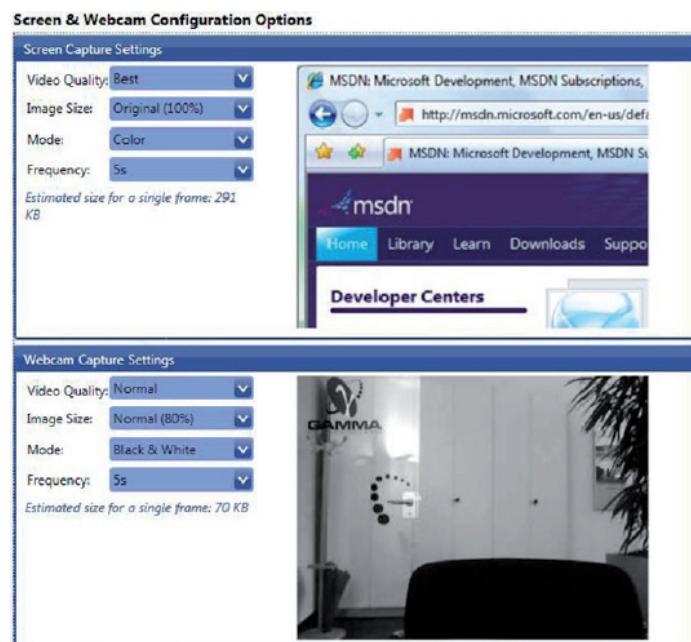
واجهة بینية سهلة الاستخدام



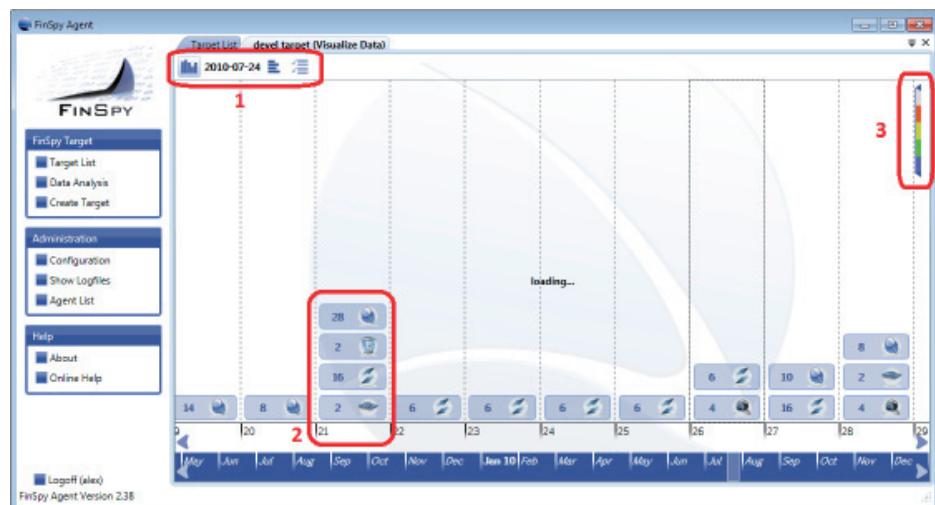
حلول المراقبة والتلويث عن بعد

FINSPY

تشكيل مباشر وغير مباشر للنظام المستهدف



جمع المعلومات الاستخباراتية على النظام المستهدف



١. بيانات مختلفة
٢. تحليل منظم للبيانات
٣. مستويات الأهمية لملفات المسجلة كلها

حلول المراقبة والتلویث عن بعد

FINSPY

موجز

يحتوي حل FinSpy ثلاثة أنواع من تراخيص المنتج

ث. ترخيص المستهدف

يتحكم ترخيص المستهدف بعدد مستهدفين FinSpy الذين يمكنهم أن «ينشطوا» بالتزاري.

النشاط هو تنشيط تركيبات مستهدفة FinSpy أكان النظام المستهدف متصلًا بالشبكة أم لم يكن.

عندما يتم نشر **FinSpy Target** على نظام مستهدف في غياب ترخيص المستهدف، يتوقف نشاط **FinSpy Target** مؤقتاً ويستحيل القيام بأي تشغيل أو النفاذ المباشر. وما إن يتتوفر ترخيص جديد (من خلال تحديث الترخيص الموجود أو تطوير أحد مستهدفين **FinSpy الناشطين**) يمنح المستهدف الترخيص المجاني وينشط فوراً بالعمل وينتتج النفاذ المباشر.

أ. ترخيص تحديث

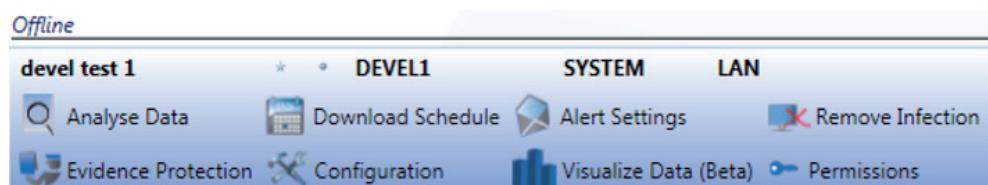
يعنى ترخيص التحديث بقدرة **FinSpy** على استعادة التحديثات الجديدة من خادم **Gamma** الخاص بالتحديثات. وهو مدمج بوحدة دعم **FinFisher™** بعد البيع. بعد انتهاء صلاحيته يبقى النظام شغالاً غير أنه لا يمكن من اكتساب الإصدارات الجديدة وبرمجيات إصلاح الأخطاء من خادم **FinSpy** الخاص بالتحديثات.

ب. ترخيص العميل

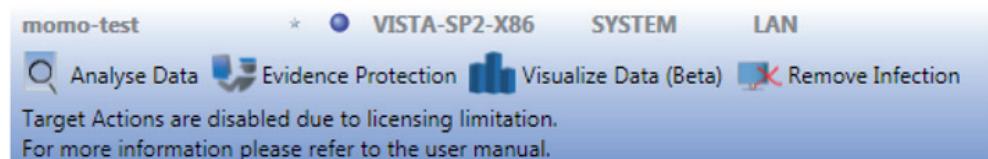
يتتحكم ترخيص العميل بعدد عمالء **FinSpy** الذين يمكنهم الولوج إلى **FinSpy Master** بالتزاري. مثلاً:

• يتم شراء ٥ تراخيص للعميل.
• يمكن تركيب تراخيص العميل من **FinSpy** على عدد غير محدود من الأنظمة ولكن ٥٠ أنظمة **FinSpy Agent** فقط تستطيع الدخول إلى **FinSpy Agent** واستخدام البيانات في الوقت نفسه.

شاشة تظهر مستهدفاً ناشطاً حائزًا ترخيصاً



شاشة تظهر مستهدفاً غير ناشط ومن دون ترخيص



حلول المراقبة والتلویث عن بعد

FINSPY MOBILE

معلومات سريعة	
عمليات استراتيجية	الاستخدام:
عمليات تكتيكية	القدرات:
مراقبة الهواتف النقالة عن بعد Microsoft Mobile Blackberry · Symbian · iPhone Android · Maemo	المحتوى:
برمجيات وتجهيزات	

مثال الاستخدام ٢ : الجريمة المنظمة
بهدف تعقب تحركات المستهدف بدقة، تم نشر FinSpy Mobile على جهاز نقال لأحد المستهدفين. وكان الحل في إرسال إشارة GPS أو تحديد هوية أبراج الهاتف الخلوية في كل ٥ دقائق إلى مقر الحكومة.

بهذه الطريقة يمكن تعقب تحركات المستهدف وتتبعها.

- الكمبيوتر المستهدف - أمثلة عن المميزات:
- اعتراض الاتصالات الأساسي (الاتصالات ورسائل SMS و MMS)
- اعتراض تام للبريد الإلكتروني
- تعقب الموقع (GPS وبيانات Cell ID)
- المراقبة المباشرة من خلال اتصالات صامتة (silent calls)
- يعمل على الهواتف العادية كلها (Blackberry و Symbian و Windows Mobile و Google Android و iPhone و Maemo)

للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج

FinSpy Mobile هو نظام تلویث ومراقبة الهواتف النقالة الذي يمكن أن تستعين به الوكالات الحكومية لمراقبة الأجهزة النقالة بصمت.

FinSpy Mobile مثالى للحالات التي لا يمكن فيها الوصول إلى شبكة شركات الهاتف أو حيث لا يكون الاعتراض غير المباشر عملياً أو حيث يكون محدوداً بسبب التشفير وعدم إمكانية الوصول.

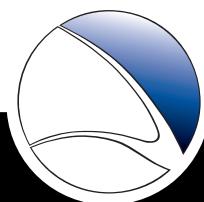
بعد أن يتم تلویث الهاتف النقال بـ FinSpy Mobile يمكنه أن يجمع البيانات ويرسلها إلى خادم FinSpy Mobile كما يمكنه أن يعترض الاتصالات الصوتية ويتيح الاستئناف إلى محيط المستهدف. يستقبل FinSpy Mobile مجموعة كاملة من أوامر التحكم مما يتاح تشكيل الجهاز عن بعد.

مثال الاستخدام ١ : وكالة استخباراتية

تم تنزيل FinSpy Mobile على جهاز Blackberry كانت فيه خاصيتنا Messaging و BlackBerry Mail مشفرتين بواسطة خادم البحث في الحركة (RIM). في هذه الحالة، يضمن FinSpy Mobile ولوجاً تاماً إلى الاتصالات الهاتفية والرسائل القصيرة وتحديد الموضع عبر نظام GPS ورسائل GPS وبريد BlackBerry بصيغة غير مشفرة.

لمحة شاملة على المميزات

- المقر - أمثلة عن المميزات:
- إدارة المستخدمين وفقاً لتصاريح الأمان
- قرة على التسجيل الصوتي (حتى ٤ × ٤)
- يمكن إدماجها بسهولة بوظيفية LEMF
- واجهة بينية للاستفسار لبيانات النظام كافة
- البحث عن الكلمات الأساسية والموضع وأرقام الهاتف
- يصدر تقارير بصيغتي RTF و PDF و PDF
- ولوج مستخدمين متعددين وفقاً للحماية الأمنية بناء على حقيقة المستخدم
- إرسال البيانات المجمعة بالبريد الإلكتروني
- إرسال رسالة قصيرة لتسجيل الإشارات المرجعية
- إرسال رسائل تحكم قصيرة للأجهزة الفردية



حلول المراقبة والتلویث عن بعد

FINSPY MOBILE

عناصر المنتج



خادم بيانات FinSpy النقال

واجهة رسومية للجلسات المباشرة والتشكيل وتحليل البيانات
الخاصة بالمستهدفين

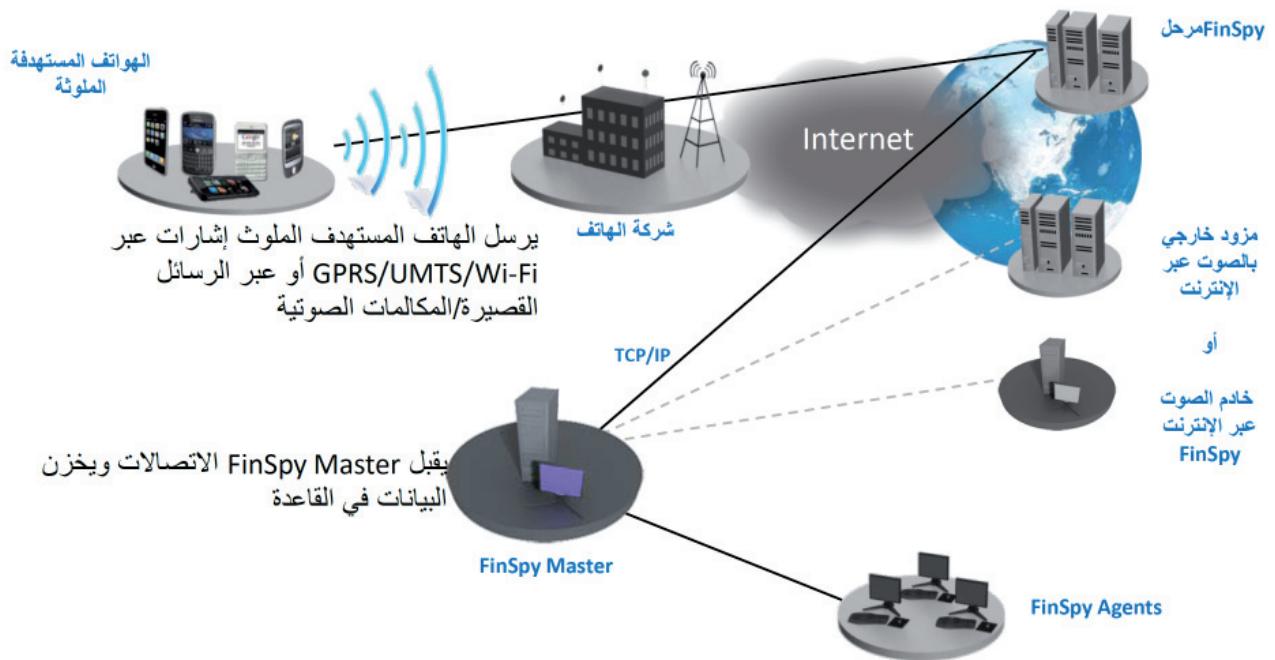
خادم Mobile Finspy لاعتراض الاتصالات

- تحكم كامل بالأنظمة المستهدفة
- حماية الإثباتات لسجلات البيانات والنشاطات
- تخزين آمن
- إدارة المستخدمين والمستهدفين القائمة على تصاريح الأمان

حلول المراقبة والتلویث عن بعد

FINSPY MOBILE

الولوج إلى أنظمة الكمبيوتر المستهدفة حول العالم



واجهة مستخدم ببنية سهلة الاستخدام

Screenshot of the FINSPY MOBILE Event Report interface, showing a list of communication events.

Header menu:

- Target Account
- Configure
- Event Report
- Remote Command
- License
- Custom Report
- Logout (admin)

Toolbar:

- All
- Call
- SMS
- IM (selected)
- Media
- Thumbnail
- Email
- Location
- Download
- Search
- Contact

Print and Refresh buttons are also visible.

Data table:

All Results											
ALL (20)											
Select	Flag	Entry	Type	Direction	Contact	Duration	Details	Mobile Time	Server Time		
	40	Im	Outgoing	User <phoenix@email.com>			[Details]	2010-October-06 02:28:05	2010-October-13 06:11:05		
	39	Im	Outgoing	User <phoenix@email.com>			[Details]	2010-October-06 02:28:05	2010-October-13 06:11:05		
	38	Im	Incoming	Phoenix <phoenix@email.com>			[Details]	2010-October-06 02:28:05	2010-October-13 06:11:05		
	37	Im	Outgoing	User <phoenix@email.com>			[Details]	2010-October-06 02:28:05	2010-October-13 06:11:05		
	36	Im	Incoming	Phoenix <phoenix@email.com>			[Details]	2010-October-06 02:28:05	2010-October-13 06:11:05		
	35	Im	Incoming	Phoenix <phoenix@email.com>			[Details]	2010-October-06 02:28:05	2010-October-13 06:11:05		
	34	Im	Incoming	Phoenix <phoenix@email.com>			[Details]	2010-October-06 02:28:05	2010-October-13 06:11:05		



حلول المراقبة والتلویث عن بعد

FINFLY USB

معلومات سريعة	
عمليات تكتيكية	الاستخدام:
نشر حل مراقبة عن بعد على الأجهزة المستهدفة	القدرات:
تجهيزات	المحتوى:

يتيح **FinFly USB** طريقة سهلة الاستخدام وموثوقة لتركيب حل مراقبة عن بعد على أنظمة الكمبيوتر حين يكون الولوج الجسدي ممكناً.

يقوم **FinFly USB** بتركيب البرمجيات المشكلة تقائياً عند إدخاله إلى الكمبيوتر مع تدخل بسيط من المستخدم أو من دونه، كما أن استخدامه في العمليات لا يتطلب علماً يتمتعون بخبرة في تكنولوجيا المعلومات. يمكن استخدامه مع أنظمة متعددة قبل إعادةه إلى المقر.

مثال الاستخدام ٢ : أمن تكنولوجيا المعلومات

تم تزويد مخبر في مجموعة إرهابية محلية بـ **FinFly USB** لتركيب حل مراقبة عن بعد سرّاً على أنظمة الكمبيوتر متعددة للمجموعة إذ استخدمت الأداة لتبادل المستندات بين أفرادها. ثم تمت مراقبة الأنظمة المستهدفة عن بعد من المقر وأعاد المخبر .FinFly USB

مثال الاستخدام ١ : وكالة استخباراتية

في بلدان عديدة، تم استخدام **FinFly USB** لتركيب حل مراقبة عن بعد سرّاً في مقاهي الإنترنت ومراكز الأعمال وذلك بكل بساطة من خلال إدخال الجهاز إلى الأنظمة المستهدفة لتتم مراقبتها عن بعد كما هو مطلوب.

لمحة شاملة على المميزات

- يقوم بتركيب حل المراقبة عن بعد سرّاً عند إدخاله إلى النظام المستهدف
- تدخل بسيط/لا تدخل من قبل المستخدم
- يمكن إخفاء الوظيفية من خلال تسجيل ملفات عادية عليه مثل الملفات الموسيقية والفيديو وغير ذلك..
- التجهيزات هي عبارة عن جهاز USB عادي الشكل وغير مشكوك بأمره

للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حلول المراقبة والتلویث عن بعد

FINFLY USB

عناصر المنتج



الدمج الكامل لـ FinSpy

- التوليد والتغليف التلقائي من خلال FinSpy Agent

FinFly USB ٠

- جهاز USB لتوثيق البرمجيات SanDisk (١٦ جيغابايت)
- ينشر حل مراقبة عن بعد عند إدخاله إلى نظام مستهدف

GAMMA INTERNATIONAL
المملكة المتحدة



هاتف: ٤١١ - ٣٣٢ ٤٤٤ - ١٢٦٤
فاكس: ٤٢٢ - ٣٣٢ ٤٤٤ - ١٢٦٤

info@gammagroup.com

المعلومات التي يحويها هذا المستند سرية وهي عرضة للتغيير من دون إشعار مسبق. Gamma Group International غير مسؤولة عن الأخطاء التقنية أو التحريرية ولا عن أي معلومات محفوظة من هذا المستند.

حلول المراقبة والتلویث عن بعد

FINFLY LAN

معلومات سريعة	
عمليات تكتيكية	الاستخدام:
ينشر حل المراقبة عن بعد في النظام المستهدف على الشبكة المحلية	القدرات:
برمجيات	المحتوى:

من بين التحديات الكبيرة التي تواجهها الوكالات الحكومية، هي المستهدفين المتنقلين نظراً إلى استحالة الولوج الجسدي إلى نظام الكمبيوتر الخاص بهم و عدم فتح ملفات ملوثة أرسلت إلى حساباتهم عبر البريد الإلكتروني. بشكل عام يعتبر المستهدفون الذين يتمتعون بالتوسيعية الأمنية هدفاً يستحيل تلویثه بما أنهم يحافظون على حداثة أنظمتهم ولا تنجح معهم أي برمجيات اختراع أساسية.

تم تصميم FinFly LAN ينشر سرّ حل المراقبة عن بعد في الأنظمة المستهدفة في الشبكة المحلية (السلكية واللاسلكية/٨٠٢،١١). هو قادر على تلویث الملفات التي ينزلها المستهدف فوراً أو على تلویث المستهدف من خلال إرسال تحديثات مزيفة للبرمجيات الأكثر شيوعاً.

مثال الاستخدام ٢ : مكافحة الفساد

تم استخدام FinFly LAN للقيام، بعاديًّا، بتركيب حل المراقبة عن بعد على كمبيوتر أحد المستهدفين بينما كان يستخدمه في غرفته في الفندق. قام العملاء الذين كانوا في غرفة أخرى، بالاتصال بالشبكة نفسها وتحكموا بالموقع الإلكترونية التي كان المستهدف يزورها وذلك لإطلاق عملية التركيب.

مثال الاستخدام ١ : وحدة مراقبة تقنية

أمضت وحدة مراقبة تقنية أساييع تتبع مستهدفاً من دون أن تتمكن من الولوج جسدياً إلى جهاز الكمبيوتر خاصته. استخدمت هذه الوحدة FinFly LAN لتركيب حل المراقبة عن بعد على كمبيوتر المستهدف بينما كان يستخدم نقطة اتصال لاسلكي (Hotspot) عامة في أحد المقاهي.

لمحة شاملة على المميزات

- يكشف أنظمة الكمبيوتر كلها الموصولة إلى الشبكة المحلية
- يعمل في الشبكات السلكية واللاسلكية (٨٠٢،١١)
- يمكن دمجه مع عدة FinIntrusion للولوج سراً إلى الشبكة
- يخفى حل المراقبة عن بعد في تنزيارات المستهدفين
- يبيّث حل المراقبة عن بعد على شكل تحديث للبرمجيات
- يقوم بعاديًّا، بتركيب حل المراقبة عن بعد من خلال الموقع الإلكترونية التي يزورها المستهدف

للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حلول المراقبة والتلویث عن بعد

FINFLY LAN

عناصر المنتج



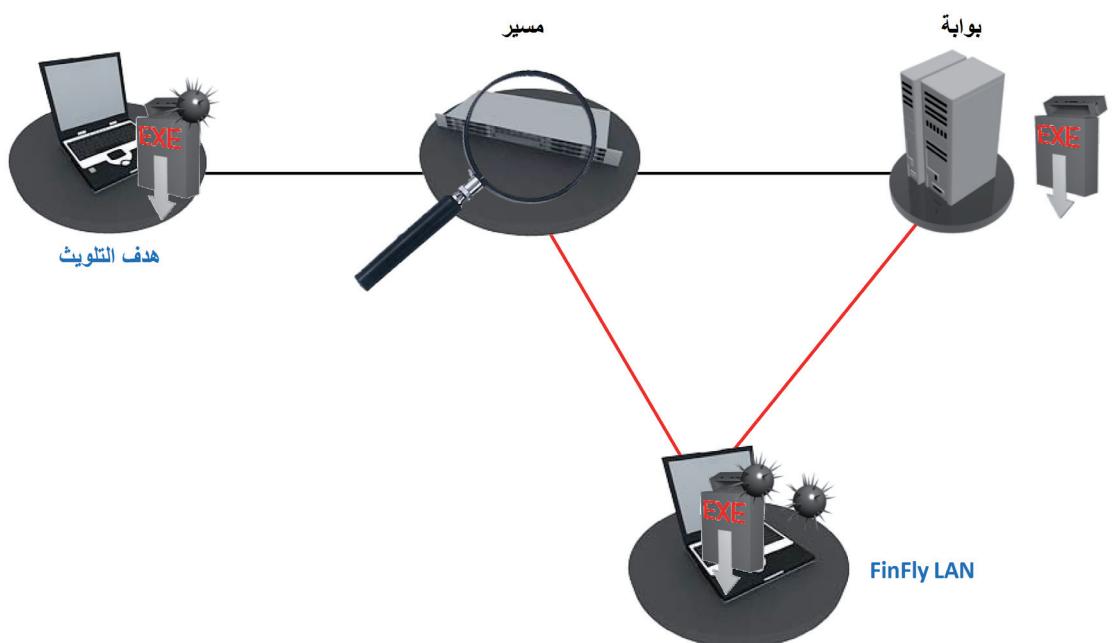
عدة FinIntrusion – الدمج (الزامي)

- يمكن إطلاق FinFly LAN كرجلة في عدة

FinFly LAN

- برمجيات تعتمد على نظام Linux مزودة بواجهة مستخدم بينية سهلة الاستخدام

التلویث من خلال الشبکات المحلیة



المراقبة عن بعد وحلول التلویث

FINFLY LAN

واجهة بینية مؤتمتة

- سهلة الاستخدام من دون تدريب عميق

Systems Infected			
Target identifier	Payload	InfectionMethod	Infected at
testuser5	test_trojan_1.exe	Binary	20:30:12 27/08/2010
10.0.0.52	test_trojan_2.exe	Update	16:12:37 23/08/2010

استيعاب مستهدفين متعددين وملفات قابلة للتنفيذ

- يمكن إضافة ملف واحد قابل للتنفيذ لكل مستهدف

Infection Techniques

Binary Infection(.exe,.scr)

Operation mode:

www.microsoft.com

enter a website's address
(eg. www.microsoft.com)



حلول المراقبة والتلویث عن بعد

FINFLY WEB

معلومات سريعة	
عمليات استراتيجية	الاستخدام:
ينشر حل المراقبة عن بعد في النظام المستهدف من خلال المواقع الإلكترونية	القدرات:
برمجيات	المحتوى:

مثال الاستخدام ٢ : وكالة استخباراتية
نشر العميل **FinFly ISP** ضمن المزود الأساسي بخدمة الإنترنت في بلاده، وكان مرفقاً بـ **FinFly Web** لتلویث المستهدفين الذين يزورون المواقع الإلكترونية الحكومية الهجومية، عن بعد، وذلك من خلال القيام سراً ببث رمز **FinFly Web** في المواقع الإلكترونية المستهدفة.

من بين التحديات الأساسية التي يواجهها مستخدمو حل المراقبة عن بعد، ذكر تركيبه في النظام المستهدف، وذلك خصوصاً عند اقتصار المعلومات على عنوان بريدي وعدم إمكانية الولوج الجسدي.

FinFly Web مصمم لإتاحة التلویث السري عن بعد لنظام مستهدف من خلال مجموعة واسعة من الهجمات المعتمدة على الويب.

في **FinFly Web**واجهة بينية سهلة الاستخدام «أشر وانقر» تتيح للعميل تشكيل رمز تلویث مكيف وفقاً لزجل مختار.

يتم تلویث الأنظمة المستهدفة التي يزور مستخدموها موقعًا مجهزاً برمز التلویث المحضر، سراً بواسطة البرمجيات المشكلة.

مثال الاستخدام ١ : وحدة المراقبة التقنية

بعد تحديد مواصفات أحد المستهدفين، أنشأت الوحدة موقعاً إلكترونياً يهمه وأرسلت له الوصلة عبر لوحة مناقشة. عند فتح الوصلة التي تقود إلى الموقع الإلكتروني للوحدة، تم تركيب حل المراقبة عن بعد على النظام المستهدف كما تمت مراقبة المستهدف من المقر.

لمحة شاملة على المميزات

- زجل وب قابلة للتكييف كلياً
- يمكن تركيبه سراً في أي موقع إلكتروني
- اندماج تام مع **FinFly ISP** و **FinFly LAN** ليتم نشره حتى ضمن مواقع إلكترونية مألفة مثل البريد الإلكتروني وبوابات الفيديو وغيرها
- قادر على تركيب حل المراقبة عن بعد حتى لو اقتصرت المعلومات على العنوان البريدي
- إمكانية استهداف كل شخص يزور المواقع الإلكترونية المشكلة

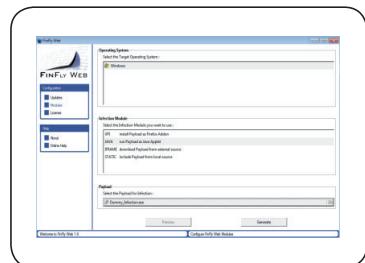
للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حلول المراقبة والتلویث عن بعد

FINFLY WEB

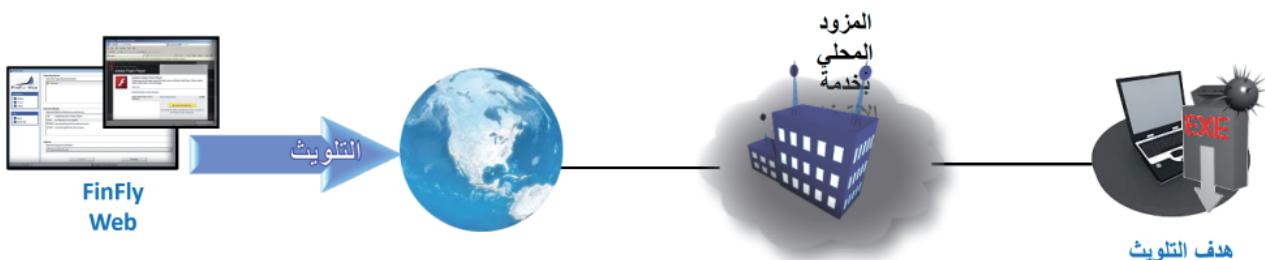
عناصر المنتج



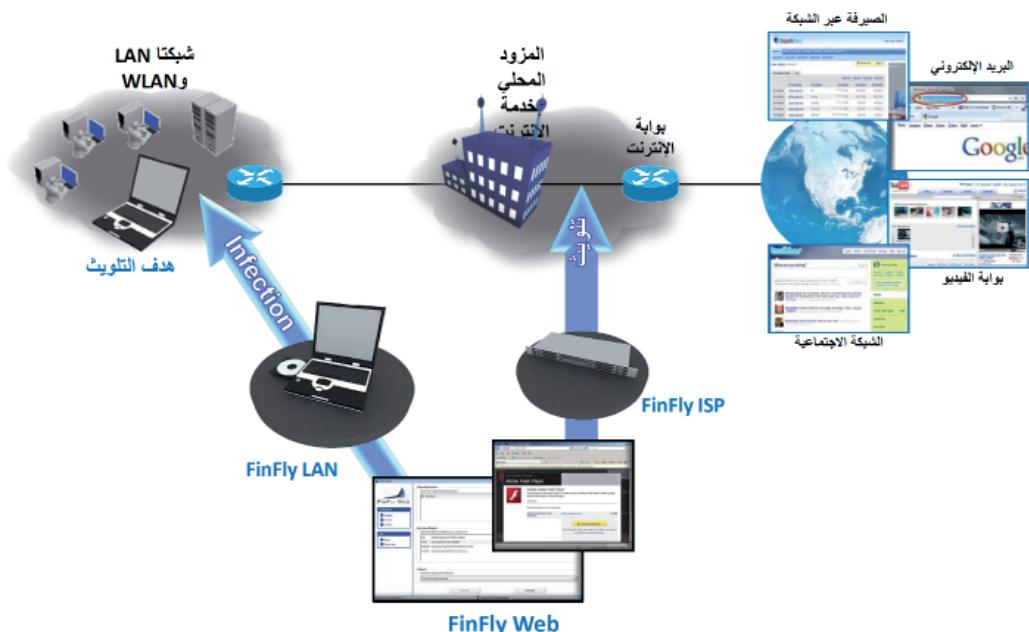
FinFly Web

برمجيات «أشر وانقر» لإنشاء موقع إلكتروني مكيفة للتلویث

التلویث المباشر بواسطة FinFly Web



اندماج كامل مع FinFly ISP و FinFly LAN



حلول المراقبة والتلوث عن بعد

FINFLY WEB

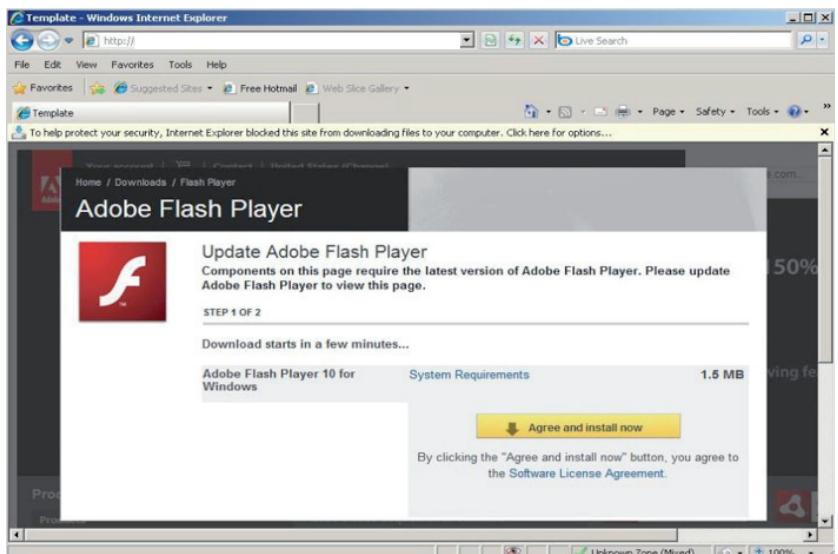
مثال: برامجات جافا (Safari، Opera، Firefox و Internet Explorer)

يدعو الموقع الإلكتروني المستهدف إلى قبول برنامج مساعدة جافا الذي قد يحمل اسم أي شركة (شركة Microsoft مثلًا)



مثال: عنصر غير موجود (Internet Explorer، Firefox، Opera، Safari)

يظهر على الموقع الإلكتروني أن برنامج المساعدة/حزم الترميز إلخ... غير موجودة على النظام المستهدف، ويدعوه إلى تنزيل هذه البرمجيات وتركيبها

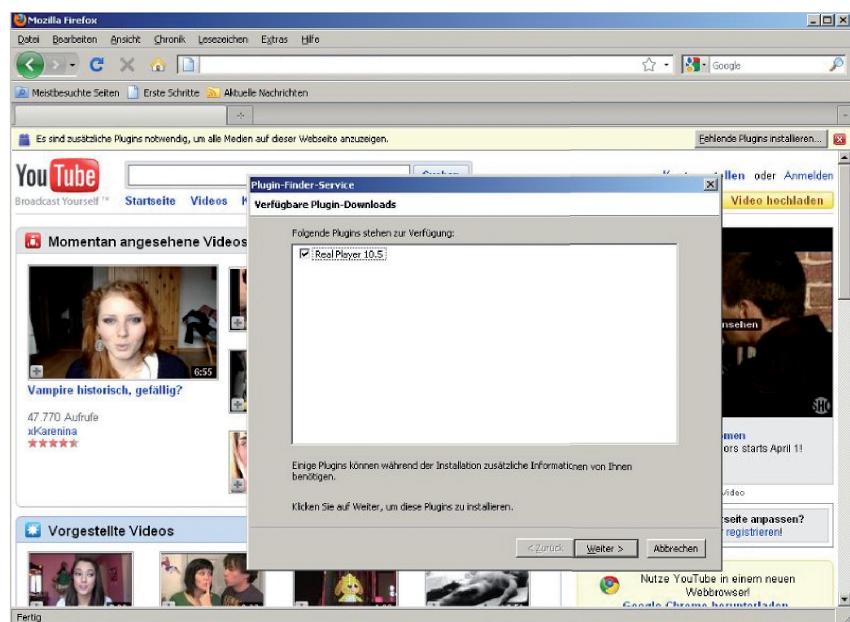


حلول المراقبة والتلویث عن بعد

FINFLY WEB

مثال: XPI غير موجود (FireFox فقط، المنصات كلها)

تدعو هذه الزجلة المستهدف إلى تركيب برمجيات معاونة إضافية للتمكن من تصفح الموقع الإلكتروني.



GAMMA INTERNATIONAL
المملكة المتحدة



هاتف: ٢٣٢ ٤١١ - ١٢٦٤ - ٤٤ +
فاكس: ٢٣٢ ٤٢٢ - ١٢٦٤ - ٤٤ +

info@gammagroup.com

المعلومات التي يحويها هذا المستند سرية وهي عرضة للتغيير
من دون إشعار مسبق. Gamma Group International.
غير مسؤولة عن الأخطاء التقنية أو التحريرية ولا عن أي معلومات
محفوفة من هذا المستند.

حلول المراقبة والتلویث عن بعد

FINFLY ISP

معلومات سريعة	
عمليات استراتيجية	الاستخدام:
نشر حل مراقبة عن بعد في النظام المستهدف من خلال شبكة المزود بخدمة الإنترنت.	القدرات:
برمجيات وتجهيزات	المحتوى:

جهاز FinFly ISP قادر على تلویث الملفات التي ينزلها المستهدف فوراً أو على تلویث المستهدف من خلال إرسال تحديثات مزيفة للبرمجيات الأكثر شيوعاً.

مثال الاستخدام: وكالة استخباراتية

تم نشر FinFly ISP في الشبكات الأساسية للمزود بخدمة الإنترنت في البلاد وقد تم استخدامه لنشر حل مراقبة عن بعد بعدياً على الأنظمة المستهدفة. وطالما أن المستهدفين المسؤولين على شبكة DSL ولهم عناوين IP ديناميكية، يمكن تحديدهم مع اسم الولوج .Radius

في العديد من العمليات، يستحيل القيام بالولوج الجسدي إلى الأنظمة المستهدفة داخل البلاد وثمة حاجة إلى تركيب حل مراقبة عن بعد بعدياً وسراً، من أجل التمكن من مراقبة الهدف من المقر.

FinFly ISP هو حل استراتيجي وعالمي وتكتيكي (نقال) يمكن دمجه في مدخل مزود خدمة الإنترنت وأو الشبكة المركزية للتنكر من تركيب حل المراقبة عن بعد، بعدياً على الأنظمة المستهدفة المختارة.

يتيح FinFly ISP للوكالات الموكلة تطبيق القانون الاطلاع على البيانات التي لا يمكنها الحصول عليها عبر الطرق الكلاسيكية لمراقبة الاتصالات عن بعد، مثلًا بسبب التشفير المستخدم قبل الولوج إلى شبكة الإنترنت أو لأن البيانات لا يمكن إرسالها عبر شبكة الإنترنت (مثلًا على ذلك، دفاتر العناوين والملفات الخاصة والجدوال الزمنية، إلخ).

ترتكز أدوات FinFly ISP على تكنولوجيا خادم موثوقة ذات قدرات هائلة يعتمد عليها لمواجهة أي تحدٌ مرتبط بتطبيقات الشبكة. مجموعة كبيرة من الواجهات البينية للشبكة – وهي كلها مزودة بوظائف اجتياز- متوفرة لترابطية الشبكة الناشطة المطلوبة.

إن العديد من الطرق السلبية والناشطة لتحديد المستهدف – بدءاً من المراقبة على الشبكة عبر التنصت السلبي وصولاً إلى التواصلي التفاعلي بين FinFly ISP وخوادم AAA- تؤكد بأنه قد تم تحديد المستهدفين وبأن تبادلاتهم قابلة للتلویث.

لمحة شاملة عن المميزات

- يمكن تركيبه داخل شبكة المزود بخدمة الإنترنت
 - يستوعب البروتوكولات الشائعة كافة
 - يختار المستهدفين وفقاً لعنوان بروتوكول الإنترنت أو اسم الولوج . Radius
 - يخفى حل المراقبة عن بعد في تنزيلات المستهدفين
 - يبتُ حل المراقبة عن بعد على شكل تحديث للبرمجيات
 - يقوم بعدياً، بتركيب حل المراقبة عن بعد من خلال المواقع الإلكترونية التي يزورها المستهدف
- للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة ميزات المنتج.

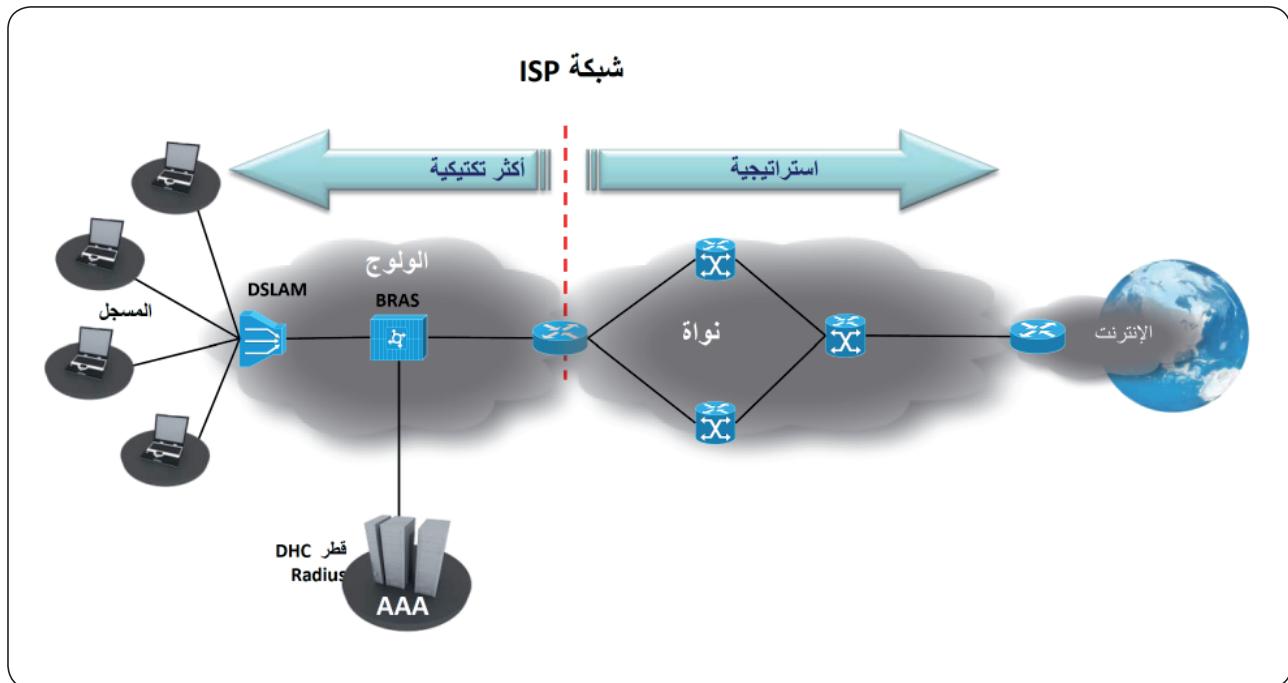


حلول المراقبة والتلویث عن بعد

FINFLY ISP

الموقع المحتملة المختلفة

يمكن استخدام FinFly ISP كحل تكتيكي أو استراتيجي داخل شبكات المزود بخدمة الإنترنت



إن هذا الحل الاستراتيجي هو تركيب FinFly ISP في شبكة المزود بخدمة الإنترنت على الدوام لاختيار وتلویث أي مستهدف عن بعد من المقر ، من دون الحاجة إلى أن تكون الوكالة الموكلة تطبيق القانون في الموقع.

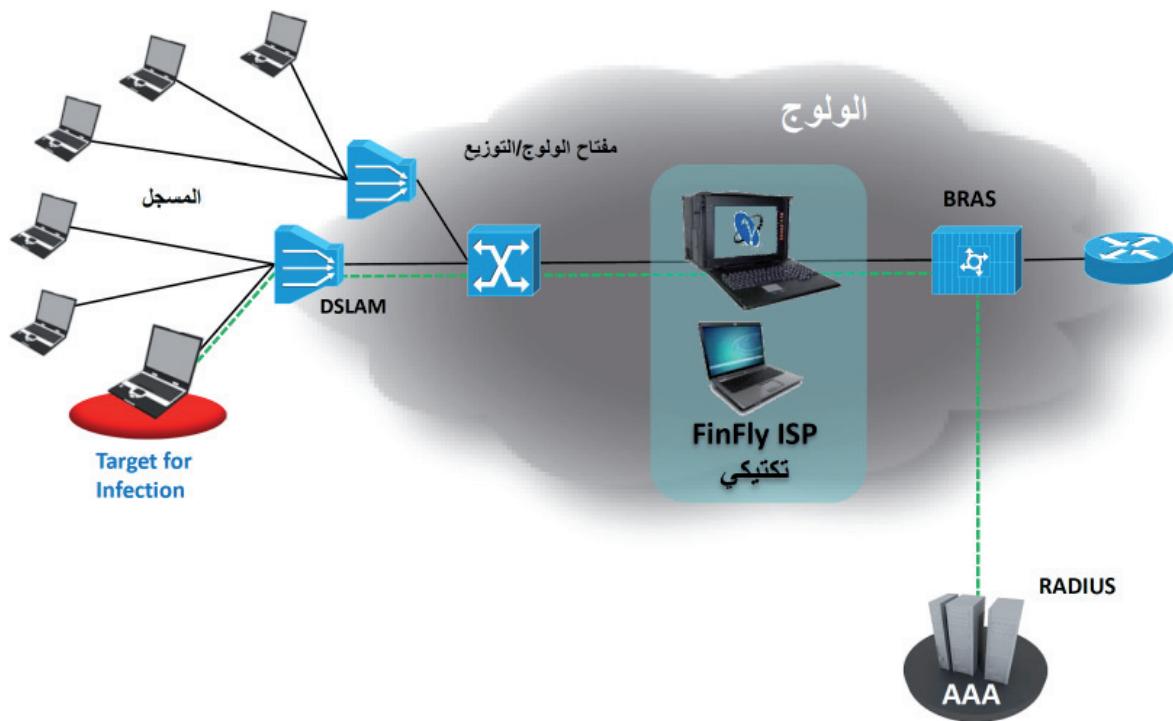
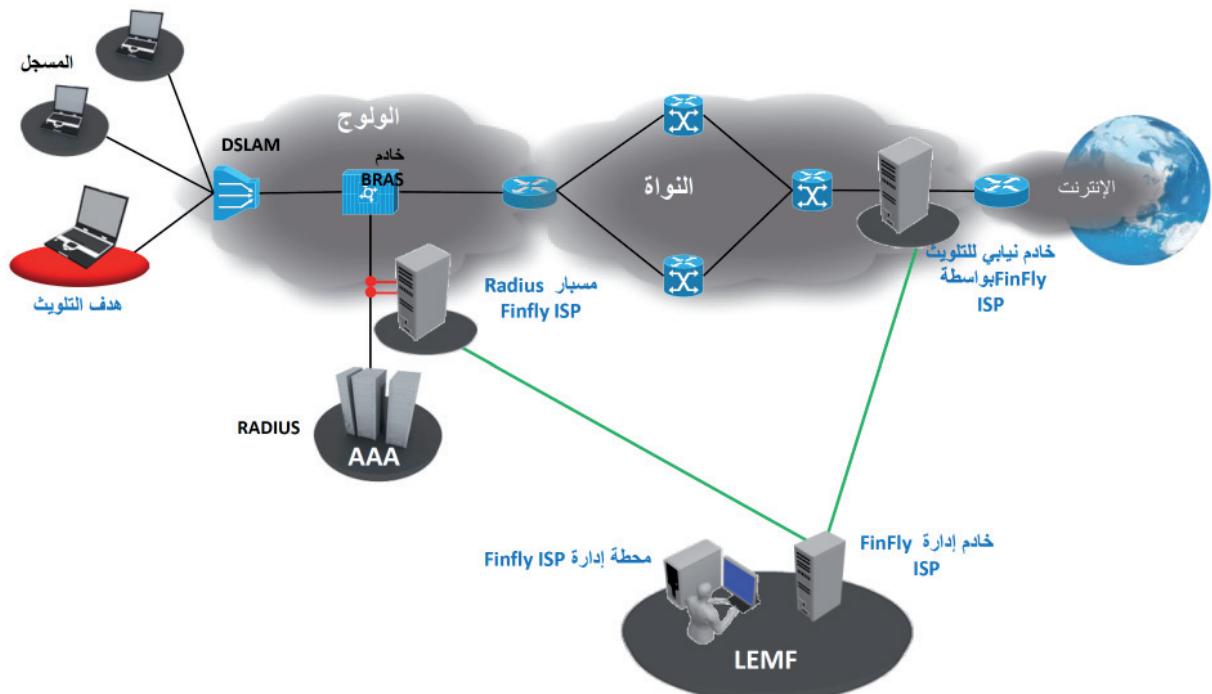
بالطبع يمكن دمج الحلول التكتيكية والاستراتيجية معًا لاستمثال مرونة عمليات التلویث.

إن هذا الحل التكتيكي نقل والتجهيزات مخصصة لمهام التلویث داخل شبكة الوصول القريبة من نقاط وصول المستهدف. يمكن نشر هذا الحل على المدى القصير لتوفير المتطلبات التكتيكية المرتكزة على مستهدف معين أو على مجموعة صغيرة من المستهدفين في منطقة ما.

حلول المراقبة والتلویث عن بعد

FINFLY ISP

إعداد الشبكة



حلول المراقبة والتلویث عن بعد

FINFLY ISP

< 20 جيغابايت في الثانية	الإنتاجية:
8 - 2	العدد الأقصى لبطاقات واجهة الشبكة:
1GE 1 نحاس/ألياف 10GE 1 نحاس/ألياف SONET/SDH OC – 3/-192 STM-1/-64 ATM AAL5	الواجهات البينية:
، Intel XEON ×8 ×1 معالج ثانٍ للنواة أو ثماني النواة	أجهزة المعالجة:
12 جيغابايت - 1 تيرابايت ذاكرة الوصول العشوائي:	
4.8TB SAS 146×3 جيغابايت سعة القرص الصلب:	
HP iLO 3 طاقة زائدة مراوح وظيفة تحويل التجاوز (في حال كان ذلك ممكناً)	المزايا:
Linux GNU (Debian 5.0)	نظام التشغيل:

عناصر المنتج

جهاز FinFly ISP الاستراتيجي

- يتطلب نشر FinFly ISP الاستراتيجي ما يلي:
- نظام الإدارة في الوكلات الموكلة تطبيق القانون
 - خادم (خوادم) تحديد المستهدف في نظام AAA على الشبكة
 - خادم (خوادم) نيابي للتلویث في بوابة (بوابات) الإنترن特.



5 جيغابايت في الثانية	الإنتاجية:
3	العدد الأقصى لبطاقات واجهة الشبكة:
1GE 1 نحاس/ألياف SONET/SDH OC – 3/-12 STM-1/-4 ATM AAL5	الواجهات البينية:
✓ Intel Core i _x 2 معالج سداسي النواة	أجهزة المعالجة:
12 جيغابايت ذاكرة الوصول العشوائي:	
1×2 SATA 1 تيرابايت سعة القرص الصلب:	
DVD+/-RW SATA محرك القرص الضوئي:	
1×17 TFT بوصة 17 المرافق:	
وظيفة تحويل التجاوز لبطاقات واجهة الشبكة	المزايا:
Linux GNU (Debian 5.0)	نظام التشغيل:

جهاز FinFly ISP التكتيكي

- يتتألف نظام FinFly ISP التكتيكي ما يلي:
- خادم نيابي نقل للتلویث وتحديد المستهدفين
 - حاسوب نظام الإدارة



إن البيانات/المميزات التقنية قابلة للتغيير من دون إشعار مسبق

GAMMA INTERNATIONAL
المملكة المتحدة



هاتف: +44 111 332 1264 - فاكس: +44 111 332 422

info@gammagroup.com

المعلومات التي يحويها هذا المستند سرية وهي عرضة للتغيير من دون إشعار مسبق. Gamma Group International غير مسؤولة عن الأخطاء التقنية أو التحريرية ولا عن أي معلومات محفوظة من هذا المستند.

حلول المراقبة والتلویث عن بعد

FIN SUPPORT

FinSupport

FinLifelineSupport

يقدم FinLifelineSupport دعماً مهنياً للمكتب الخافي لحل المشاكل والاستفسارات التقنية. كذلك يوفر دعماً للمكتب الخافي عن بعد تصحيح أخطاء FinFisher™ SW و استبدال التجهيزات بموجب كفالة. بالإضافة إلى ذلك، يحصل الزبون تلقائياً على المميزات والوظائف الجديدة مع وظيفة تصحيح الأخطاء.

تصحيح الأخطاء

FinSupport هو عبارة عن منظمة لدعم المنتجات حيث يتولى مدير دعم يتمتع بكافأة عالية تلقي الاستفسارات عبر البريد الإلكتروني أو الهاتف من الزبائن بعد البيع. يكون مركز مدير خدمات ما بعد البيع في ألمانيا وساعات عمله هي التالية: ٩:٠٠ - ١٧:٠٠ (توقيت وسط أوروبا).

لذلك فإن خدمات الدعم متوفرة من الساعة ٩:٠٠ وحتى الساعة ١٧:٠٠ (توقيت وسط أوروبا)، وفي حال تم تقديم طلب للحصول على الدعم بعد ساعات العمل المذكورة، يتم تلبيتها فوراً في يوم العمل التالي.

عندما يبلغ الزبون عن حصول حادث، يتم تقديم تقرير عن حادث وتوثيق مدى أولوية هذا الحادث. وفي خلال وقت محدد، يتم اتخاذ الإجراءات التصحيحية الازمة وذلك وفقاً لأولوية المحددة. ويتوالى فريق FinFisher™ عندها مسؤولية التحقيق في تقرير الحادث وحله بالإضافة إلى إبلاغ معد تقرير الحادث بالوضع والمعلومات الجديدة.

في ما يتعلق بالمسائل ذات الأولوية العالية، نحن نضمن بأن النظم ما زال يعمل بشكل جيد من خلال تقديم حلول مؤقتة وتصحيح المشاكل والأخطاء. لدى تقديم فريق العمل الحل المؤقت يقوم في الوقت نفسه بتقديم تقرير المشكلة إلى قسم البحث والتطوير لضمان حل المشكلة بسرعة. تساهم إجراءات الدعم الاحترافية هذه في ضمان أن هذه البرمجيات تلبي أعلى التوقعات.

يبين المخطط الانسيابي التالي الإجراءات التشغيلية المعهودة ومناطق المسؤولية (ملاحظة: في هذا المخطط الانسيابي، يمثل «الزبون» معد تقرير الحادث).

يحافظ جهاز FinSupport على تحديثات منتجات FinFisher™ مع عقد سنوي بتقديم خدمات الدعم.

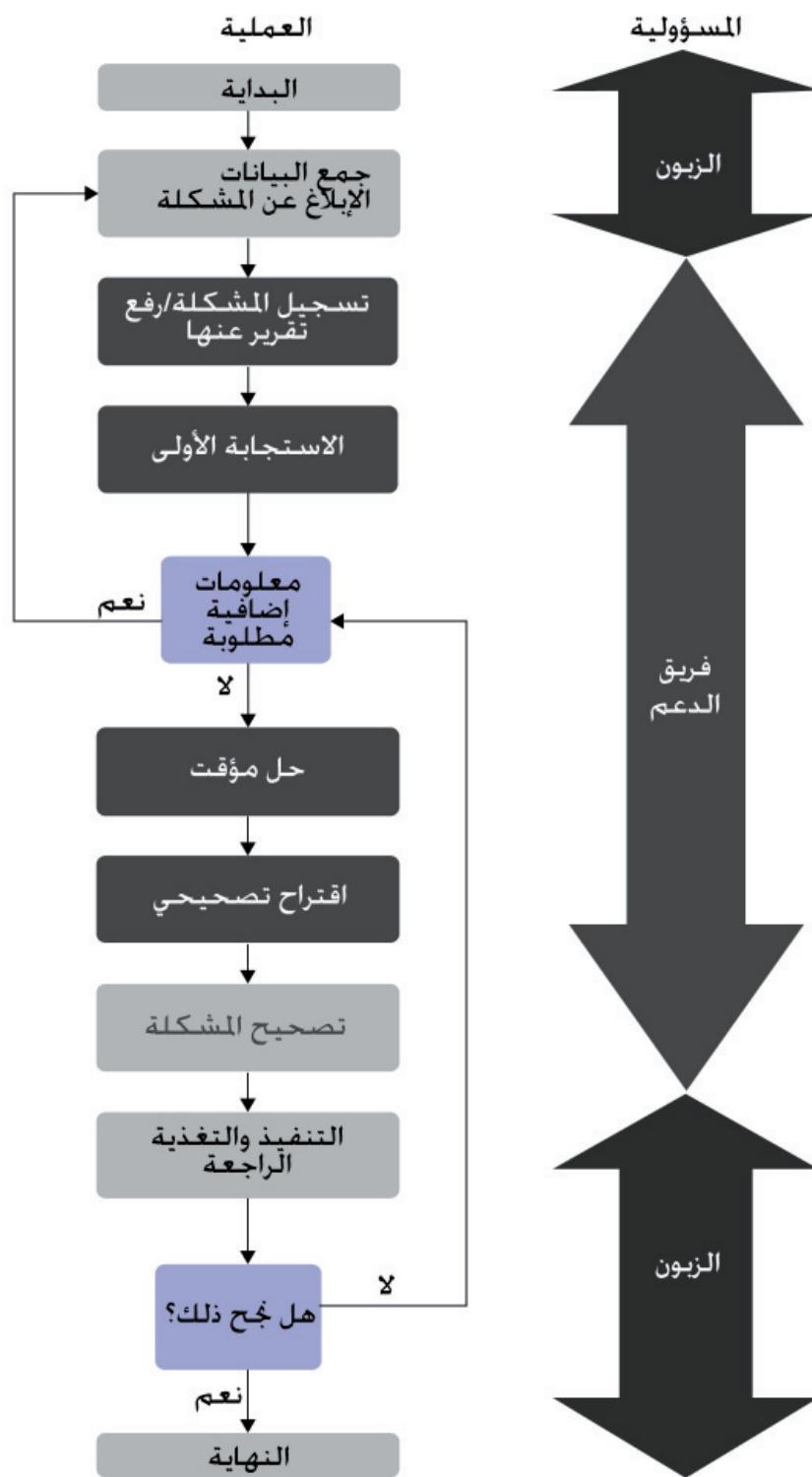
وتعرض صفحة FinFisher™ الإلكترونية الخاصة بالدعم، الخدمات التي يقدمها فريق الدعم وهي التالية:

- الولوج على الشبكة إلى:
- دليل المستخدم الأخير
- مميزات المنتج الأخيرة
- حصص التدريب على المنتج الأخيرة
- واجهة أمامية للإبلاغ عن الأخطاء
- واجهة أمامية لطلب المميزات
- تحديثات البرمجيات الدورية:
- تصحيح الأخطاء
- مميزات جديدة
- إصدارات مهمة جديدة
- دعم تقني من خلال برنامج skype
- تصحيح الأخطاء
- دعم تشغيلي جزئي



حلول المراقبة والتلويث عن بعد

FIN SUPPORT



حلول المراقبة والتلویث عن بعد

FIN SUPPORT

يظهر الجدول التالي الإجراءات العادلة المتّبعة لمعالجة الحوادث التي يعلن عنها الزبون

الزبون	معالجة تقرير الحادث والمهام
في حال ظهور أي شوائب (مشكوك بها) في التجهيزات/البرمجيات، إحصل على تقرير الحادث وفقاً لإحدى الطرق المحددة. ويتعين أن يشمل تقرير الحادث: <ul style="list-style-type: none">- معلومات عن العقد- اسم الزبون- النظام/التقنية الذي يعاني من شائبة- وصف الشائبة- الأولوية (انظر التعريف أدناه)- مؤشرات الخطأ الظاهرة	خصصت FinFisher™ بريداً إلكترونياً ورقم هاتف/فاكس للتقارير عن الحوادث.
تعاون الزبون يكون من خلال تقديم مؤشرات إضافية عن الخطأ عند الطلب.	في خلال يوم واحد، يحصل الزبون على رقم التذكرة لتأكيد الاستلام ويتابع تقرير الحادث كما ونتائج التحليل الأولى.
تقديم FinLifelineSupport عملية جمع مؤشرات المشكلة عند الطلب.	تدعم FinLifelineSupport اقتراحات تصحيحاً لتقرير الحادث
يُتضمن إجراءات تصحيحية مخطط لها ووقت الاستجابة وتحليل ما بعد الحادث.	تقديم FinLifelineSupport مسألة تعديل التجهيزات أو البرمجيات في حال كان الحادث المبلغ عنه يستوجب الإصلاح.
يطبق الزبون تعديلات التجهيزات/البرمجيات. يؤكد الزبون نجاح العملية.	تساعد FinLifelineSupport في تطبيق تعديلات التجهيزات*/ البرمجيات

* في حال عدم وجود أي ضمانات، تتحسب التجهيزات على حدة.



حلول المراقبة والتلوث عن بعد

FINSUPPORT

تتولى FinLifelineSupport معالجة الشكاوى والمشاكل التي تتناقها وذلک وفقاً لمدى خطورتها. ثمة عاملان أساسيان لتصنيف خطورة الحادث، وهما موجودان في كل تقرير حادث.

- «أولوية» ترتكز فقط على نطاق الخطأ التقني
- «سوء استعمال الزبون» وهو عامل أكثر موضوعية يرتكز على الزبون.

يعرض جدول «الأولوية» التالي لمحة عامة عن النطاق التقني المعنى:

الأولوية	التعريف	المثال
١	مشكلة أساسية: جانب مهم في النظام لا يعمل	البرنامج النبائي معطل ولا يمكن التواصل مع مستهدف FinSpy
٢	مشكلة كبيرة من دون حل مؤقت	التقط برنامج إدارة الفيروسات برمجية RMS مركبة سابقاً وهي تتطلب تحديثاً فورياً لتبقى ناشطة في النظام الملوث.
٣	مشكلة كبيرة مع حل مؤقت	لا يعمل برنامج Finspy المستهدف بالشكل المناسب ولكن يمكن اتباع حل مؤقت.
٤	مشكلة صغيرة لها تأثير بسيط على النظام	ظهور أيقونة خاطئة ل البرنامج تم تنزيله

وقت الاستجابة

يكون وقت «الاستجابة الأولية» منذ تاريخ تسجيل الحادث إلى تاريخ حصول الزبون على الموافقة التي تؤكّد استلام طلب الحادث. وقد تتطلب «الاستجابة الأولية» أيضاً معلومات إضافية، أو في الحالات الأقلّ تعقيداً قد تقوم بحل المشكلة على الفور.

في ٩٠ في المئة من الحالات، سبقي أوقات الاستجابة كما هو مبين في الجدول أدناه.

«يوم (أيام) العمل» = كما هو محدد في التقويم الألماني وبذلك تستثنى أيام العطل المعتمدة في ألمانيا.

ثمة ثلاثة عبارات تستخدم في أوقات الاستجابة:

- الاستجابة الأولية
- إجراءات تصحيحية
- حل المشكلة (أو تصنيف الأولويات)

حلول المراقبة والتلویث عن بعد

FIN SUPPORT

أوقات الاستجابة	الاستجابة الاولى	التغذية التصحيحة للجرائم	حل المشكلة الاولويات
الأولوية - 1 مشكلة أساسية	يوم العمل نفسه	يوم عمل واحد	يوماً عمل: ملاحظة: قد تستغرق عملية حل المشكلة وقتاً اطول وفقاً للمشكلة والابحاث المطلوبة
الأولوية - 2 مشكلة كبيرة من دون حل مؤقت	يوم العمل نفسه	يوماً عمل	خمسة أيام عمل: قد تستغرق عملية حل المشكلة وقتاً اطول وفقاً للمشكلة والابحاث المطلوبة
الأولوية - 3 مشكلة أساسية مع حل مؤقت	يوم العمل نفسه	3 أيام عمل	14 يوم عمل: قد تستغرق عملية حل المشكلة وقتاً اطول وفقاً للمشكلة والابحاث المطلوبة
الأولوية ٤ - مشكلة بسيطة	يوم العمل نفسه	7 أيام عمل	تحديث البرمجيات التالي

تحديثات البرمجيات

يشمل FinLifeLineSupport تحديثات دورية للبرمجيات ويضمن تحديثات تقافية للنظام الراهن مع خدمة تصحيح الأخطاء الصغيرة التي يتم التزويده بها من خلال نظام التحديث.

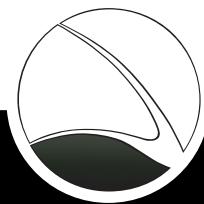
تشمل هذه التحديثات مميزات جديدة ووظائف معززة تتماشى مع متطلبات العميل (باستثناء التجهيزات).



برنامج التدريب على اختراق تكنولوجيا المعلومات

FINTRAINING

يشمل برنامج التدريب على اختراق تكنولوجيا المعلومات حصصاً حول المنتجات المتوفرة وطريقاً عملية وتقنيات لاختراق تكنولوجيا المعلومات. يضع هذا البرنامج خبرة سنوات من المعرفة في تصرف المستخدمين النهائيين ويعزز قدراتهم في هذا المجال.



FINFISHER™
IT INTRUSION

WWW.GAMMAGROUP.COM

برنامج التدريب على اختراق تكنولوجيا المعلومات

FINTRAINING

معلومات سريعة	
تبادل المعرفة	الاستخدام:
الدرائية في مجال اختراق تكنولوجيا المعلومات قدرات لمواجهة حرب الإنترن特	القدرات:
تدريب	المحتوى:

يقوم FinAdvisory بتحويل حصة تدريب فردية إلى برنامج تدريب واستشارات محترف من شأنه أن يبني أو يعزز قدرات فريق عمل اختراق تكنولوجيا المعلومات. إن حصص التدريب مكيفة تماماً وفقاً لمتطلبات المستخدم النهائي والتحديات التشغيلية التي يواجهها.

ومن أجل ضمان قابلية الاستخدام الكامل لهذه الدراسة المكتسبة، يتم توفير دعم تشغيلي داخل البلاد في خلال البرنامج.

برنامج FinAdvisory

- برنامج كامل للاستشارات والتدريب على اختراق تكنولوجيا المعلومات
- تشكيل وتدريب منظم فريق عمل اختراق تكنولوجيا المعلومات
- تقييم كامل لأعضاء الفريق
- حصص تدريب عملية تركز على العمليات الواقعية
- استشارات تشغيلية داخل البلاد

للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.

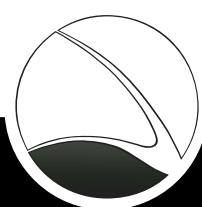
إن الوعي الأمني ضروري لأي حكومة للحفاظ على أمن تكنولوجيا المعلومات والتمكن من تجنب التهديدات التي تطال البنى التحتية لتكنولوجيا المعلومات والتي قد تؤدي إلى فقدان السرية وإلى نقص في البيانات وتوفيرها.

من جهة أخرى، إن مواضيع مثل حرب الإنترن特 والاعتراض الناشط وتجميع المعلومات الاستخباراتية عبر اختراق تكنولوجيا المعلومات، قد أصبحت أكثر أهمية في الحياة اليومية وهي تحتم على الحكومة تشكيل فرق عمل متخصصة في مجال اختراق تكنولوجيا المعلومات لمواجهة هذه التحديات الجديدة.

يتولى إعطاء حصص FinTraining خبراء عالميون في مجال اختراق تكنولوجيا المعلومات وذلك بطريقة عملية تركز على العمليات الواقعية وعلى ما يتبعه المستخدم النهائي أن يقوم به للتمكن من مواجهة التحديات اليومية التي تعرّضه.

أمثلة عن مواضيع حصص التدريب

- تحديد مواصفات الواقع الإلكتروني المستهدفة والأشخاص المستهدفين.
- تعقب البريد الإلكتروني المجهول ولوح عن بعد إلى حسابات البريد الإلكتروني
- تقييم أمن خوادم الويب وخدمات الويب
- استغلال البرمجيات عملياً
- اختراق تكنولوجيا المعلومات لاسلكياً (الشبكة اللاسلكية/ ٨٠٢,١١ والبلوتونث)
- هجمات على البنى التحتية الأساسية
- سلب البيانات واعتمادات المستخدم على الشبكات
- مراقبة نقاط الاتصال اللاسلكي ومقاهي الإنترن特 وشبكات الفنادق.
- اعتراض الاتصالات وتسجيلها (بروتوكول الصوت عبر الإنترن特 DECT و VoIP)
- استعادة كلمات المرور





GAMMA INTERNATIONAL
المملكة المتحدة



هاتف: ٢٣٢ ٤١١ - ٠٢٦٤ - ٤٤٤
فاكس: ٢٣٢ ٤٢٢ - ٠٢٦٤ - ٤٤٤

info@gammagroup.com

WWW.GAMMAGROUP.COM