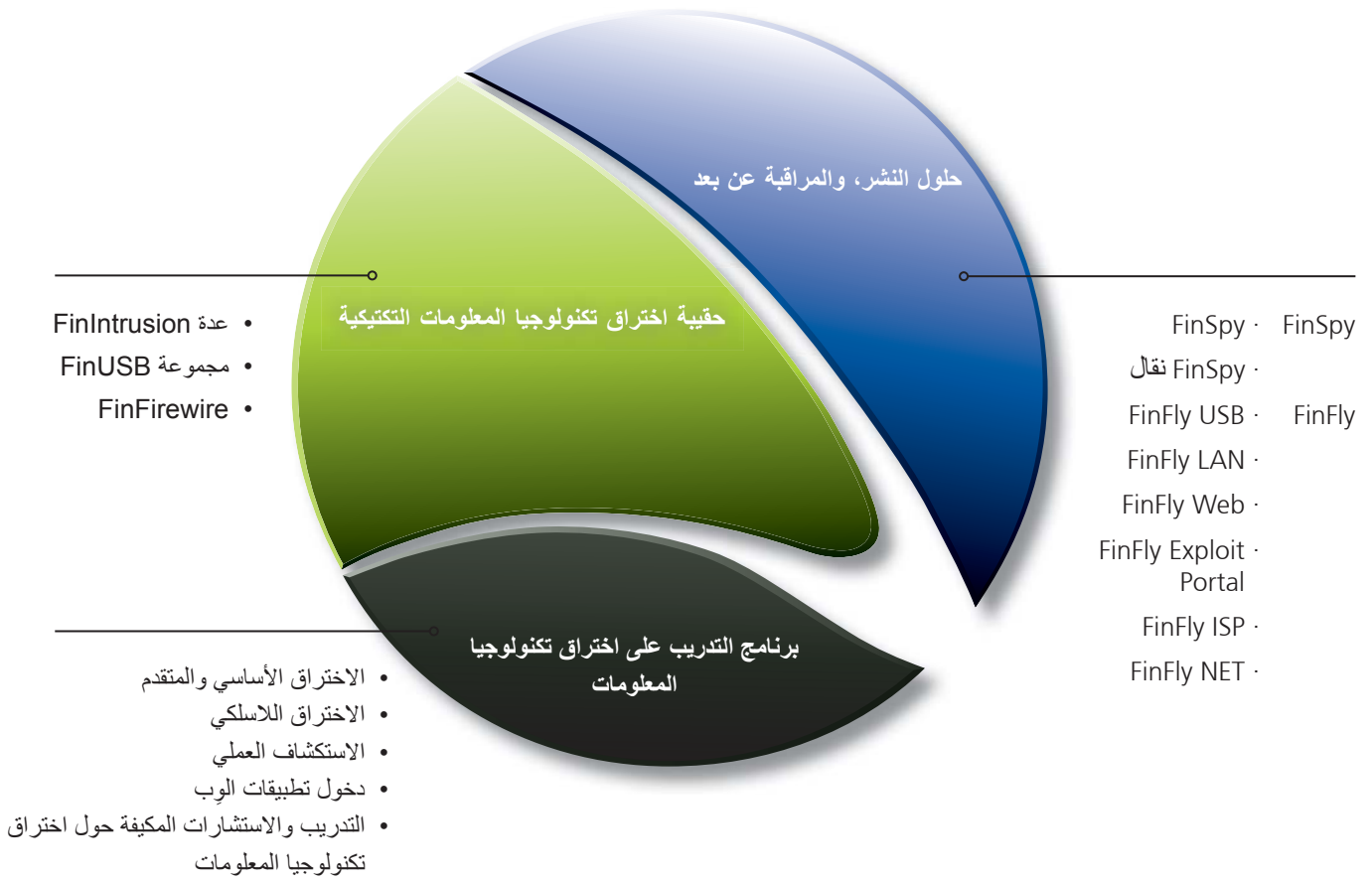


FINFISHER: حلول اختراق تكنولوجيا المعلومات
والمراقبة عن بعد للحكومات



FINFISHER™
IT INTRUSION

WWW.FINFISHER.COM



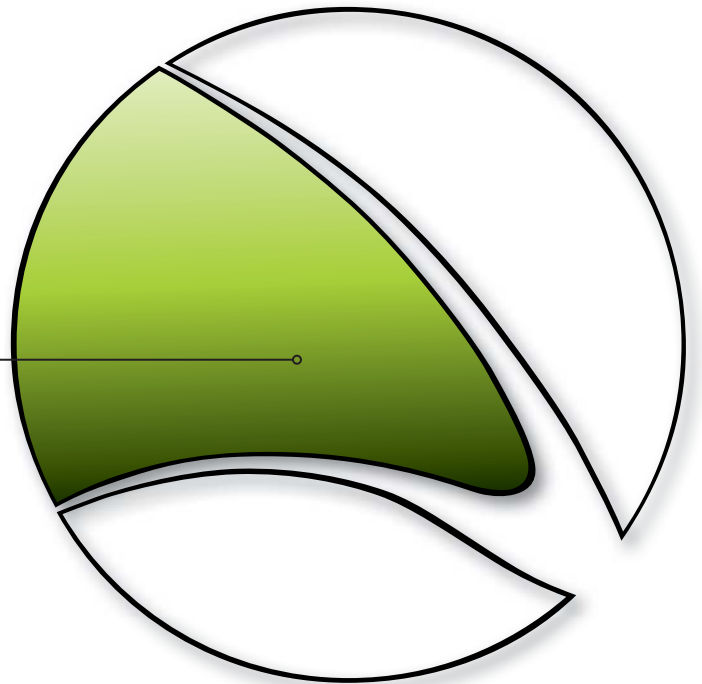
حقيبة اختراق تكنولوجيا المعلومات التكتيكية

FININTRUSION عدة

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 تكتيكياً.



حقيبة اختراق تكنولوجيا المعلومات التكتيكي

عدّة FININTRUSION

معلومات سريعة	
الاستخدام:	• عمليات تكتيكية / استراتيجية
القدرات:	• فك شفرة الخصوصية المكافئة للشبكات السلكية/ بروتوكول الوصول الآمن للشبكة اللاسلكية • مراقبة الشبكات (بما في ذلك جلسات بروتوكول SSL) • هجمات اختراق تكنولوجيا المعلومات
المحتوى:	• تجهيزات/برمجيات

عدّة 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 تقييم مستوى سلامة وأمن شبكات ومنظمات متعددة.

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

مثال الاستخدام ٢: أمن تكنولوجيا المعلومات

استخدم عملاء كثيرون عدّة FinIntrusion لتجاوز أمن بعض الشبكات وأنظمة الكمبيوتر لغايات هجومية ودفاعية باستخدام أدوات وتقنيات مختلفة.

مثال الاستخدام ٣: برمجيات استراتيجية لتقييم استجابة الأنظمة

تستخدم عدّة FinIntrusion للولوج عن بعد إلى حسابات بريد المستهدفين وإلى خوادم الويب الخاصة بهم (المدونات ومنتديات المناقشة) ولمراقبة نشاطاتهم وسجلات ولوجهم وغيرها.

مثال الاستخدام ١: وحدة المراقبة التقنية

استخدمت عدّة FinIntrusion لفك تشفير بروتوكول الوصول الآمن للشبكة اللاسلكية (WPA) لشبكة مستهدفة لاسلكية منزلية ومن ثم لمراقبة بريده الإلكتروني على الويب (Yahoo و Gmail، ...) وشبكاته الاجتماعية (Facebook و MySpace، ...). وقد تمكن ذلك المحققين من مراقبة هذه الحسابات عن بعد انطلاقاً من مقراتهم من دون أن يحتاجوا إلى الاقتراب من مستهدفهم.

لمحة شاملة على المميزات

- تكشف الشبكات اللاسلكية (٨٠٢,١١) وأجهزة البلوتوث
- تستعيد الخصوصية المكافئة للشبكات السلكية (WEP) (٦٤ و ١٢٨ بت) وعبارات المرور في غضون ٢ إلى ٥ دقائق
- تكسر عبارات مرور WPA١ و WPA٢ 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/طبقة النقل الآمن
- WiFi Catcher مدمج يمكن دمج مع وظائف مراقبة كلمة السر
- تدخل عن بعد إلى حسابات البريد الإلكتروني باستخدام تقنيات اختراق تعتمد على الشبكات أو الأنظمة أو كلمات المرور
- تقييم أمن الشبكة والتأكد عليه

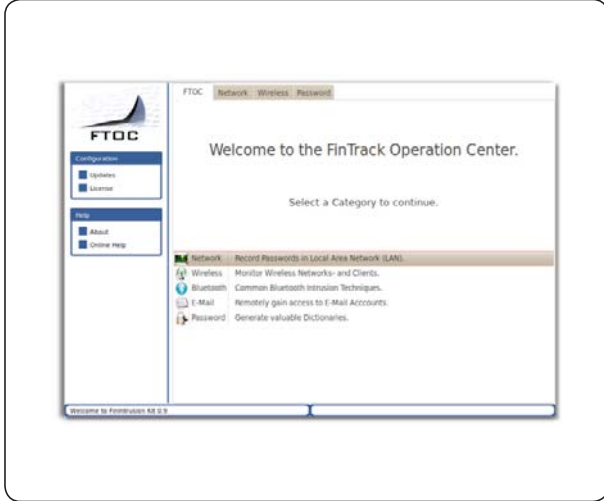
للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حقيبة اختراق تكنولوجيا المعلومات التكتيكي

عدة FININTRUSION

عناصر المنتج



مركز عمليات FinTrack

- واجهة مستخدم ببنية لهجمات اختراق تكنولوجيا المعلومات المؤتمتة



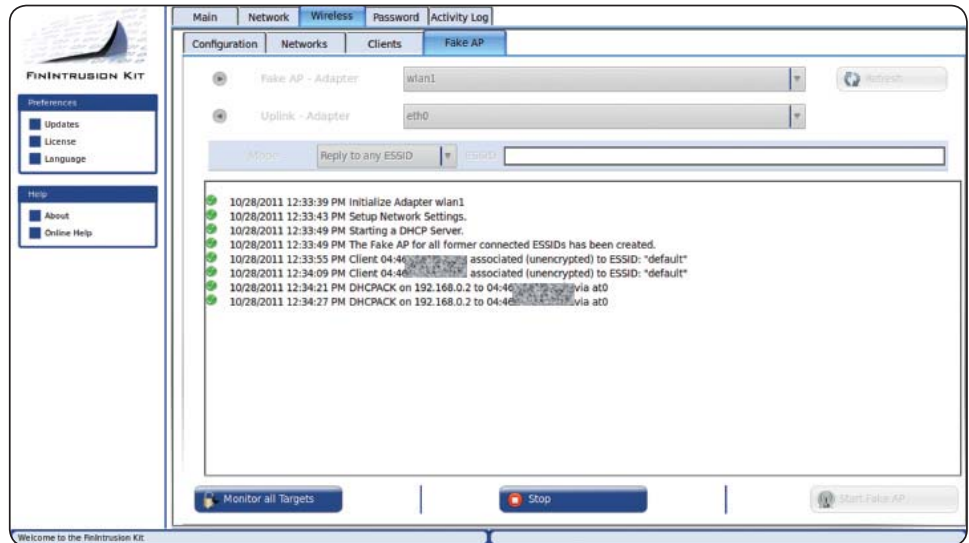
عدة FinIntrusion - وحدة تكتيكية سرية

العناصر الأساسية لاختراق تكنولوجيا المعلومات:

- مهائى WLAN بطاقة عالية
- مهائى بلوتوث بطاقة عالية
- هوائيات ٨٠٢,١١
- والكثير من الأدوات الأخرى لاختراق تكنولوجيا المعلومات

WiFi Catcher

- يلتقط أجهزة WLAN القريبة ويسجل حركة مرور الوب وكلمات السر.

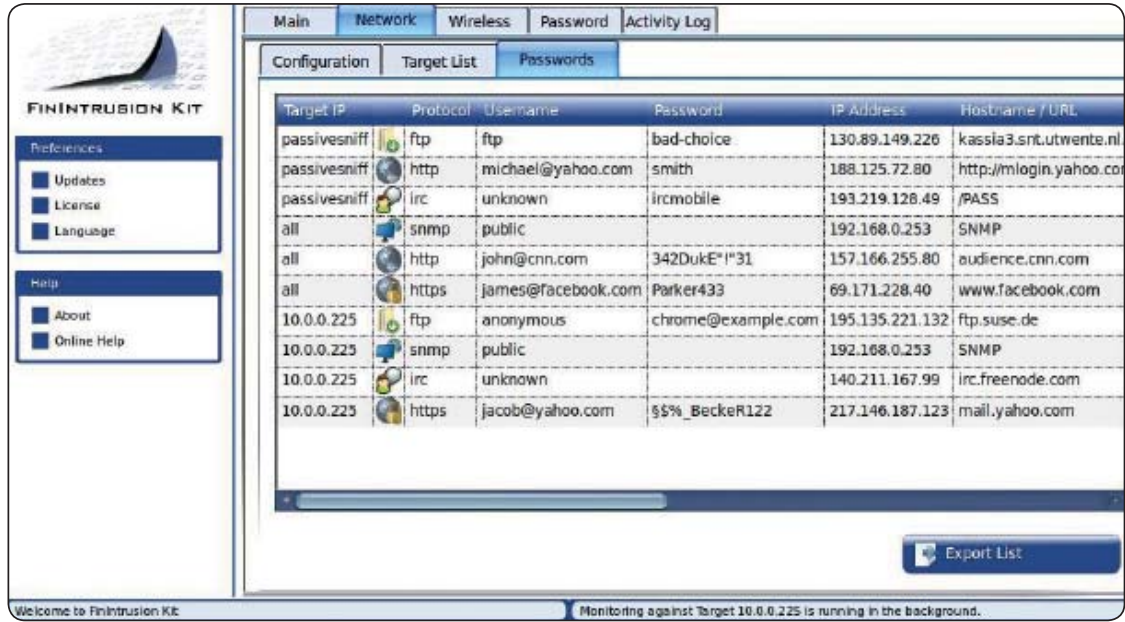


حقيبة اختراق تكنولوجيا المعلومات التكتيكية

عددة FININTRUSION

برنامج الكشف عن كلمات السر في الشبكات المحلية والشبكات اللاسلكية

- يكشف عن البيانات المشفرة بنظام أمن الاتصالات كالبريد الإلكتروني على الوب وبوابات الفيديو والصيرفة عبر الإنترنت، إلخ...



The screenshot displays the FININTRUSION KIT web interface. The main window is titled 'FININTRUSION KIT' and features a navigation menu with tabs for 'Main', 'Network', 'Wireless', 'Password', and 'Activity Log'. The 'Password' tab is active, showing a table of detected credentials. The table has columns for 'Target IP', 'Protocol', 'Username', 'Password', 'IP Address', and 'Hostname / URL'. Below the table is an 'Export List' button. The status bar at the bottom indicates 'Monitoring against Target 10.0.0.225 is running in the background.'

Target IP	Protocol	Username	Password	IP Address	Hostname / URL
passivesniff	ftp	ftp	bad-choice	130.89.149.226	kassia3.snt.utwente.nl
passivesniff	http	michael@yahoo.com	smith	188.125.72.80	http://mlogin.yahoo.co
passivesniff	irc	unknown	ircmobile	193.219.128.49	/PASS
all	snmp	public		192.168.0.253	SNMP
all	http	john@cnn.com	342Duke*!^31	157.166.255.80	audience.cnn.com
all	https	james@facebook.com	Parker433	69.171.228.40	www.facebook.com
10.0.0.225	ftp	anonymous	chrome@example.com	195.135.221.132	ftp.suse.de
10.0.0.225	snmp	public		192.168.0.253	SNMP
10.0.0.225	irc	unknown		140.211.167.99	irc.freenode.com
10.0.0.225	https	jacob@yahoo.com	\$\$%_BeckeR122	217.146.187.123	mail.yahoo.com



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

هاتف: ٤١١ ٣٣٢ ١٢٦٤ - ٤٤٤

فاكس: ٤٢٢ ٣٣٢ ١٢٦٤ - ٤٤٤

info@gammagroup.com

WWW.FINFISHER.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 محذوفة من هذا المستند.

حقيبة اختراق تكنولوجيا المعلومات التكتيكي

عدة FINUSB

معلومات سريعة	
الاستخدام:	• عمليات تكتيكية
القدرات:	• جمع المعلومات • الوصول إلى النظام • الحصول على معلومات جنائية سريعة
المحتوى:	• تجهيزات / برمجيات

مجموعة FinUSB هي عبارة عن منتج مرن يمكن الوكالات الموكله تطبيق القانون والوكالات الاستخباراتية من استخراج المعلومات الجنائية بطريقة سريعة وأمنة من أنظمة الكمبيوتر من 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 ٢: وحدة المراقبة التقنية

كانت إحدى وحدات المراقبة التقنية تتبع مستهدفاً كان يزور مقاهي إنترنت مختلفة بشكل عشوائي ما جعل من المستحيل مراقبته بواسطة تقنية شبيهة بحصان طروادة. استخدم FinUSB لاستخراج البيانات المتبقية على المنافذ العامة التي استخدمها المستهدف بعد مغادرته.

أمكن استعادة مستندات كثيرة فتحها المستهدف على بريده الإلكتروني بهذه الطريقة. وضمت المعلومات المجمعة بشكل أساسي ملفات Office أساسية وتاريخ التصفح من خلال تحليل سجلات المتصفحات وأكثر.

مثال الاستخدام ١: عملية سرية

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

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

لمحة شاملة على المميزات

- مستمثل للعمليات السرية
- سهولة الاستخدام من خلال التنفيذ الآلي
- استخراج أسماء المستخدمين وكلمات المرور الخاصة بهم للبرمجيات الشائعة مثل:
 - برامج عميل البريد الإلكتروني
 - برامج التراسل الفوري
 - المتصفحات
 - أدوات الإدارة عن بعد
- النسخ الصامت للملفات (البحث في القرص الصلب، وسلة المهملات والملفات التي فُتحت أو صُححت أو أُنشئت مؤخراً)
- استخراج معلومات خاصة بالشبكة (سجلات المحادثات وتاريخ التصفح ومفاتيح WEP/WPA (٢)...)...
- مراكمة معلومات النظام (البرمجيات العاملة/المركبة، معلومات القرص الصلب، ...)

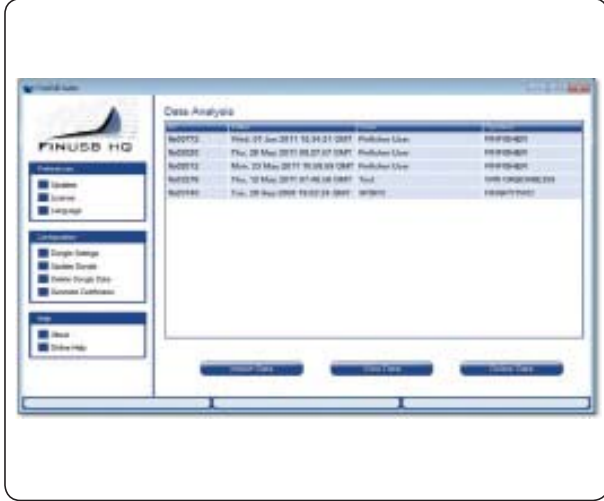
للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حقيبة اختراق تكنولوجيا المعلومات التكتيكي

عدة FINUSB

عناصر المنتج



FinUSB HQ

- واجهة مستخدم ببنية لفك شفرة البيانات المجمعَة وتحليلها
- تشكيل الخيارات التشغيلية لجهاز توثيق البرمجيات



مجموعة FinUSB - وحدة نقالة



FinUSB - تجاوز حماية كلمات المرور في Windows

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



١٠ أجهزة لتوثيق البرمجيات (U3 ١٦ جيجابايت)

- يستخرج بسرية البيانات من الأنظمة



حقيبة اختراق تكنولوجيا المعلومات التكتيكي

عدة FINUSB

سهولة الاستخدام

1. اختر جهاز FinUSB لتوثيق البرمجيات
2. قم بتشكيل المميزات/الزجل كلها التي ترغب فيها وحدث جهاز FinUSB لتوثيق البرمجيات خاصتك بواسطة FinUSB HQ
3. توجه إلى نظامك المستهدف
4. قم بوصل جهاز توثيق البرمجيات Fin USB إليه
5. انتظر حتى يتم نقل البيانات كلها
6. عد إلى FinUSB HQ
7. استورد البيانات كلها من جهاز توثيق البرمجيات FinUSB
8. أعط التقرير



تقارير احترافية



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

هاتف: ٤١١ ٣٣٢ ١٢٦٤ - ٤٤٤

فاكس: ٤٢٢ ٣٣٢ ١٢٦٤ - ٤٤٤

info@gammagroup.com

WWW.FINFISHER.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 محذوفة من هذا المستند.

حقيبة اختراق تكنولوجيا المعلومات التكتيكي

FINFIREWIRE

معلومات سريعة	
• عمليات تكتيكية	الاستخدام:
• تجاوز كلمة مرور المستخدم • الولوج السري إلى النظام • استعادة كلمات السر من الذاكرة العشوائية • إتاحة التحقيق المباشر	القدرات:
• تجهيزات / برمجيات	المحتوى:

يواجه كل من وحدات المراقبة والخبراء الجنائيون وضعاً يحتاج فيه إلى ولوج نظام كمبيوتر عامل من دون إطفائه تفادياً لفقدان البيانات أو توفيراً للوقت في خلال عملية. في معظم الحالات، تتم حماية النظام المستهدف بواسطة **حافظ شاشة مقفل بكلمة مرور** أو لا يكون المستخدم قد كتب كلمة السر ليلج إلى النظام بينما تكون **شاشة الدخول** عاملة.

يمكن FinFireWire المشغل من تجاوز الشاشة المقفلة بكلمة مرور بسرعة وسرية تامة والولوج إلى النظام المستهدف من دون ترك أي أثر أو تشويه أي إثبات جنائي.

مثال الاستخدام ٢: استعادة كلمة السر

استخدمت الوحدات الجنائية التي تستعمل المنتج مع تطبيقات جنائية تقليدية مثل Encase® وظيفية تفرغ الذاكرة العشوائية للحصول على لمحة عن معلومات الذاكرة العشوائية المتوفرة كما استعادت عبارة المرور المشفرة للقرص الصلب التي تم وضعها بواسطة برمجيات TrueCrypt التي شغرت القرص الصلب كاملاً.

مثال الاستخدام ١: العمليات الجنائية

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

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

لمحة شاملة على المميزات

- يحل أفعال 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 Windows و Mac و Linux
- يعمل مع FireWire/1394 و PCMCIA و Express Card

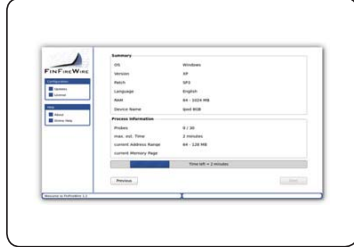
للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حقيبة اختراق تكنولوجيا المعلومات التكتيكي

FINFIREWIRE

عناصر المنتج



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



- وحدة FinFireWire التكتيكية
- نظام تكتيكي كامل



مجموعة كابلات Universal FinWire

- ٤ pin إلى ٤ pin
- ٤ pin إلى ٦ pin
- ٦ pin إلى ٦ pin




بطاقات توسعة الشبكة


- بطاقات ExpressCard وPMCIA وبطاقات FireWire
- للأنظمة المستهدفة غير المزودة بمنفذ FireWire

الاستخدام


٤. اختر مستهدفاً




٥. انتظر حتى يفتح النظام




١. توجه إلى النظام المستهدف



٢. أطلق FinFireWire



٣. قم بوصل مهائى وكابل FinFireWire



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

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

info@gammagroup.com

WWW.FINFISHER.COM

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

حلول النشر، والمراقبة عن بعد

FINSPY

FINSPY MOBILE

FINFLY USB

FINFLY LAN

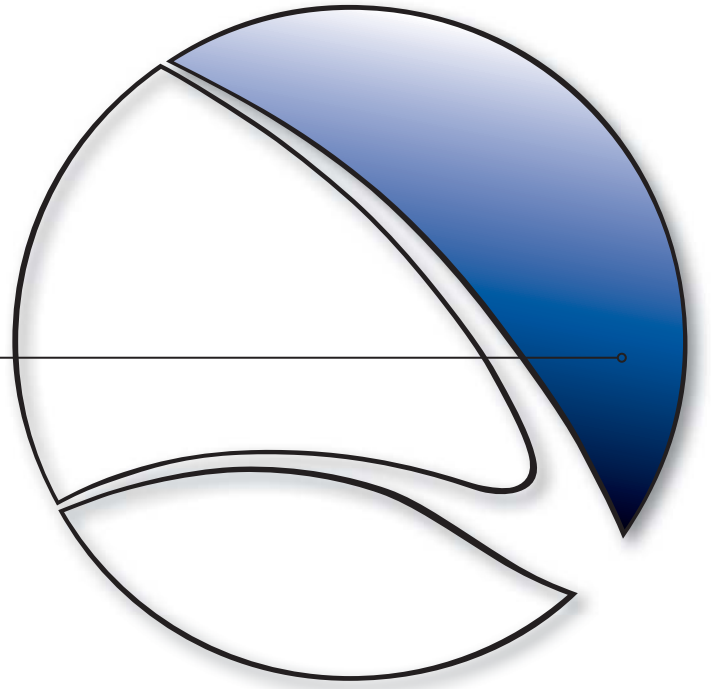
FINFLY WEB

FINFLY EXPLOIT

PORTAL

FINFLY ISP

FINFLY NET



تستخدم المراقبة عن بعد و حلول التلويث للنفاذ إلى البرامج المستهدفة وها يتيجان الولوج التام إلى المعلومات المخزنة وإمكانية التحكم بوظائف الأنظمة المستهدفة إلى حد التقاط البيانات والاتصالات المشفرة. إذا استعملت هذه الحلول مع طرق معززة للتلويث عن بعد، سنتيح للوكالات الحكومية القدرة على تلويث الأنظمة المستهدفة عن بعد.



حلول النشر، والمراقبة عن بعد

FINSPY

معلومات سريعة	
• عمليات استراتيجية / تكتيكية	الاستخدام:
• مراقبة الكمبيوتر عن بعد • مراقبة الاتصالات المشفرة	القدرات:
• برمجيات	المحتوى:

مثال الاستخدام ١: وكالة استخباراتية

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

مثال الاستخدام ٢: الجريمة المنظمة

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

المقر - أمثلة عن المميزات:

- حماية الإثباتات (إثباتات صالحة وفقاً للمعايير الأوروبية)
- إدارة المستخدمين وفقاً لتصاريح الأمان
- تشفير البيانات الأمنية وتناقلها بواسطة RSA ٢٠٤٨ و AES ٢٥٦
- بمنأى عن العامة من خلال برامج إخفاء الهوية
- يمكن إدماجه بسهولة بوظيفية LEMF

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

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 بالتوعية الأمنية ويغيرون مواقعهم باستمرار ويستعملون قنوات تواصل مشفرة ومجهولة و يقيمون في الخارج.

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

- بيانات لا تنتقل عبر أي شبكة
- عمليات تواصل مشفر
- 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 تثبيت FinSpy على نظام كمبيوتر، يمكن التحكم به عن بعد ولوجه فور وصله إلى الإنترنت/الشبكة، أينما كان النظام المستهدف في العالم.

لمحة شاملة على المميزات

الكمبيوتر المستهدف - أمثلة عن المميزات:

- تجاوز ٤٠ نظاماً مختبراً مضاداً للفيروسات
- تواصل سري مع المقر
- مراقبة Skype بالكامل (الاتصالات والدرشة ونقل البيانات والفيديو ولانحة الأسماء)
- تسجيل التواصل العادي كالبريد الإلكتروني وجلسات الدردشة والصوت عبر بروتوكول الإنترنت
- مراقبة مباشرة عبر كاميرا الويب والميكروفون
- 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
- يعمل مع غالبية أنظمة التشغيل (Windows و Mac OSX)





FinSpy Agent

- واجهة رسومية للجلسات المباشرة
- تشكيل وتحليل البيانات الخاصة بالمستهدفين

FinSpy Master ونظام نيابي

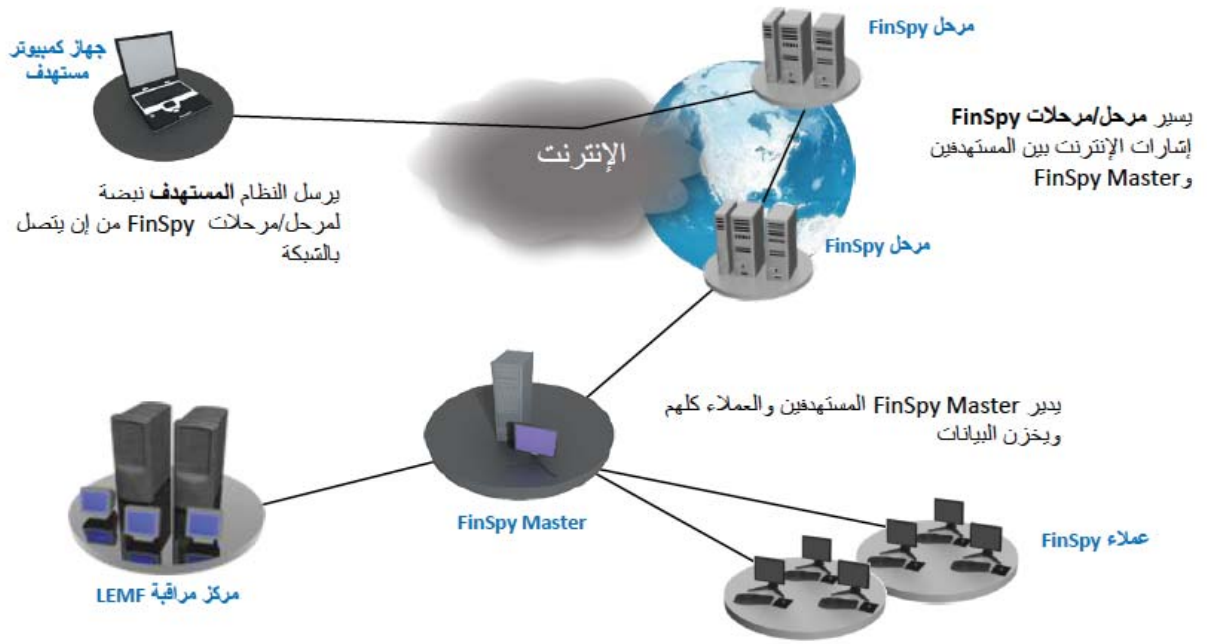
- تحكم كامل بالأنظمة المستهدفة
- حماية الإثباتات لسجلات البيانات والنشاطات
- تخزين آمن
- إدارة المستخدمين والمستهدفين القائمة على تصاريح الأمان



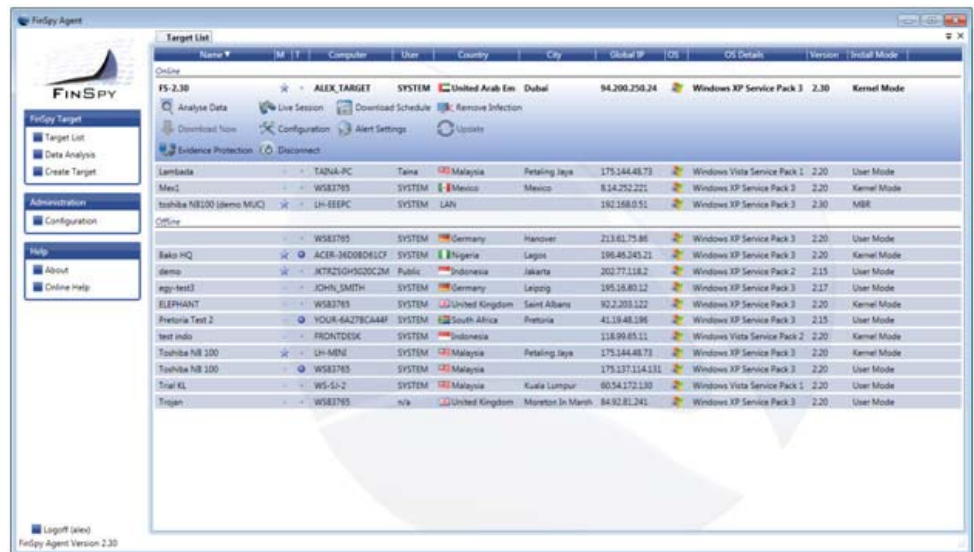
حلول النشر، والمراقبة عن بعد

FINSPY

الولوج إلى أنظمة كمبيوتر المستهدفين حول العالم



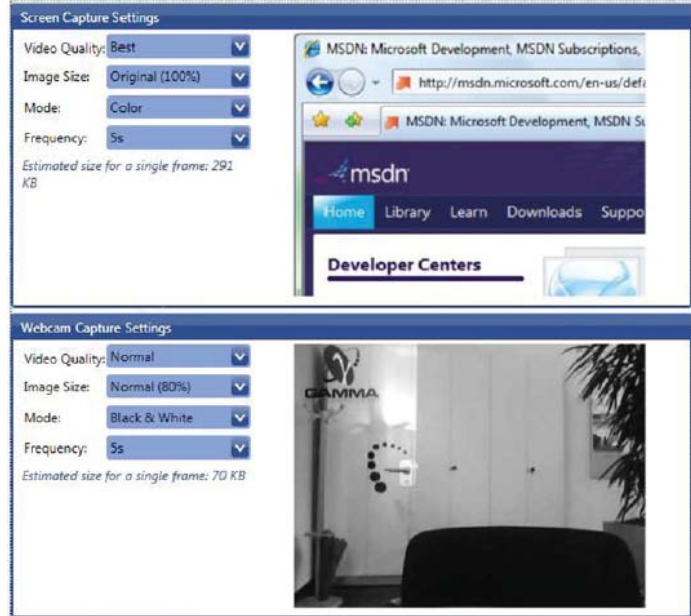
واجهة بينية سهلة الاستخدام



حلول النشر، والمراقبة عن بعد

FINSPY

تشكيل مباشر وغير مباشر للنظام المستهدف



جمع المعلومات الاستخباراتية على النظام المستهدف



1. بيانات مختلفة
2. تحليل منظم للبيانات
3. مستويات الأهمية للملفات المسجلة كلها



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

هاتف: ٤١١ ٣٣٢ - ١٢٦٤ - ٤٤٤

فاكس: ٤٢٢ ٣٣٢ - ١٢٦٤ - ٤٤٤

info@gammagroup.com

WWW.FINFISHER.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 محذوفة من هذا المستند.

حلول النشر، والمراقبة عن بعد

FINSPY MOBILE

معلومات سريعة

• عمليات استراتيجية / تكتيكية	الاستخدام:
• مراقبة الهواتف الخلوية عن بعد	القدرات:
• برمجيات / تجهيزات	المحتوى:

مثال الاستخدام ١: وكالة استخباراتية

تم نشر FinSpy Mobile على أجهزة **Blackberry** نقالة تعود لعددت مستهدفين وذلك من أجل مراقبة المحادثات جميعها بما فيها رسائل **SMS/MMS** والرسائل الإلكترونية والدردشة عبر **Blackberry**.

مثال الاستخدام ٢: الجريمة المنظمة

تم نشر FinSpy Mobile سراً في الهواتف النقالة للعديد من أفراد إحدى عصابات الجريمة المنظمة. من خلال البيانات الناتجة عن التعقب بواسطة جهاز **GPRS** والاتصالات الصامتة، تم جمع المعلومات الأساسية من كل اجتماع عقدته هذه المجموعة.

المقر- أمثلة عن المميزات:

- حماية الإثباتات (الإثباتات الصالحة وفقاً للمعايير الأوروبية)
- إدارة المستخدمين وفقاً لتصاريح الأمان
- بمنأى 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.

FinSpy Mobile مثالي للحكومات لأنه يؤمن الاعتراض ولأكثر منصات الهواتف الذكية شيوياً.

يمكن للمنظمات التي لا تتمتع بالقدرة على الاعتراض على الشبكة أو خارجها الولوج إلى الهواتف النقالة واعتراض الأجهزة. ناهيك عن ذلك يتيح هذا الحل الولوج إلى الاتصالات المشفرة وإلى البيانات المخزنة على الأجهزة والتي لا يتم تناقلها.

تواجه حلول الاعتراض التكتيكي أو الاستراتيجي تحديات لا يمكن التصدي لها إلا باستعمال أنظمة هجومية مثل FinSpy Mobile:

- البيانات التي لا يتم نقلها عبر أي شبكة والتي تحفظ على الجهاز
- الاتصالات المشفرة في الواجهة الهوائية، ما يتيح تقادي استعمال الأنظمة التكتيكية النشطة أو السلبية غير المباشرة.
- التشفير بحسب مبدأ النهاية للنهاية من الجهاز لبرامج الدردشة والرسائل الإلكترونية ورسائل PIN.

باستعمالها FinSpy Mobile ، حصلت الوكالات الحكومية التي تجمع المعلومات عن بعد من الهواتف النقالة المستهدفة، على نتائج ممتازة.

عندما يتم تثبيت FinSpy Mobile على هاتف نقال، يمكن أن يتم التحكم به ومراقبته عن بعد أينما كان المستهدف.

لمحة شاملة على المميزات

الهاتف المستهدف- أمثلة عن المميزات:

- التواصل السري مع المقر
- تسجيل الاتصالات الشائعة مثل المكالمات الهاتفية ورسائل SMS و MMS والرسائل الإلكترونية
- المراقبة المباشرة من خلال اتصالات صامتة (Silent Calls)
- تنزيل الملفات (المتصلون، الروزنامة، الصور، الملفات)
- تعقب المستهدفين داخل البلاد (Cell ID وبيانات GPS)
- تسجيل كامل للدردشة بواسطة **Blackberry Messenger**
- يعمل على أنظمة التشغيل الشائعة كلها (Windows Mobile، **Blackberry OS**، **Android** و **iOS (iPhone)** و **Symbian**)



FINSPY MOBILE

عناصر المنتج



FinSpy Agent

- واجهة بيئية رسومية للجلسات المباشرة والتشكيل وتحليل بيانات المستهدفين



Proxy و FinSpy Master

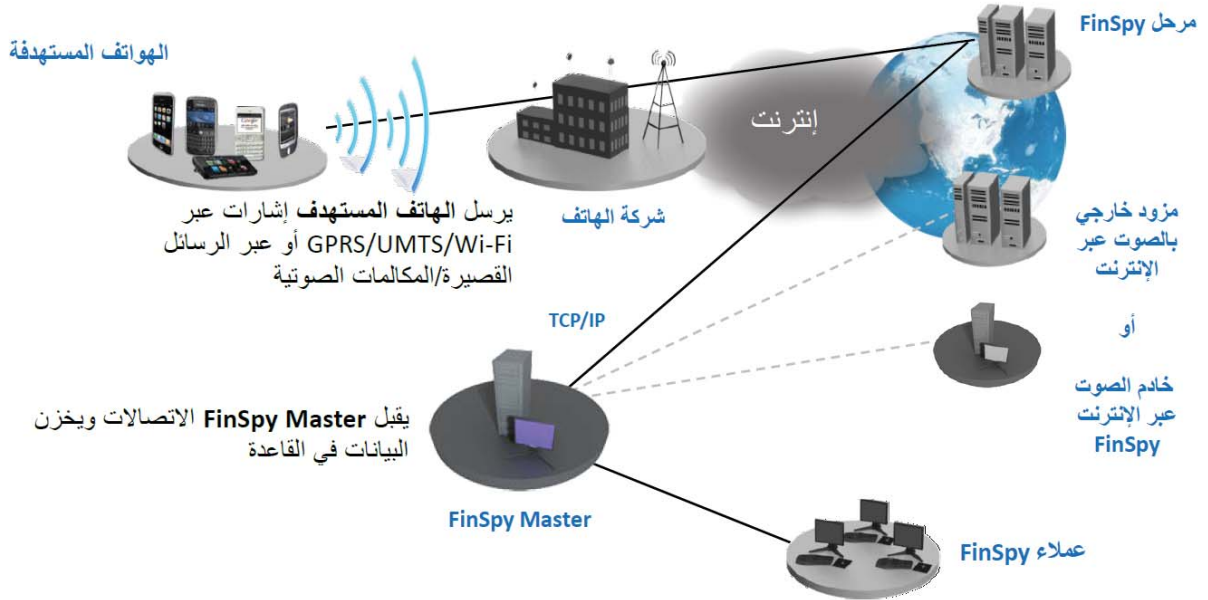
- التحكم الكلي بالهواتف المستهدفة
- حماية الإثباتات لسجلات البيانات والنشاطات
- تخزين آمن
- تصريح أمان بناءً على إدارة المستخدم والمستهدف



حلول النشر، والمراقبة عن بعد

FINSPY MOBILE

الولوج إلى أنظمة الكمبيوتر المستهدفة حول العالم



واجهة مستخدم بديهية سهلة الاستخدام

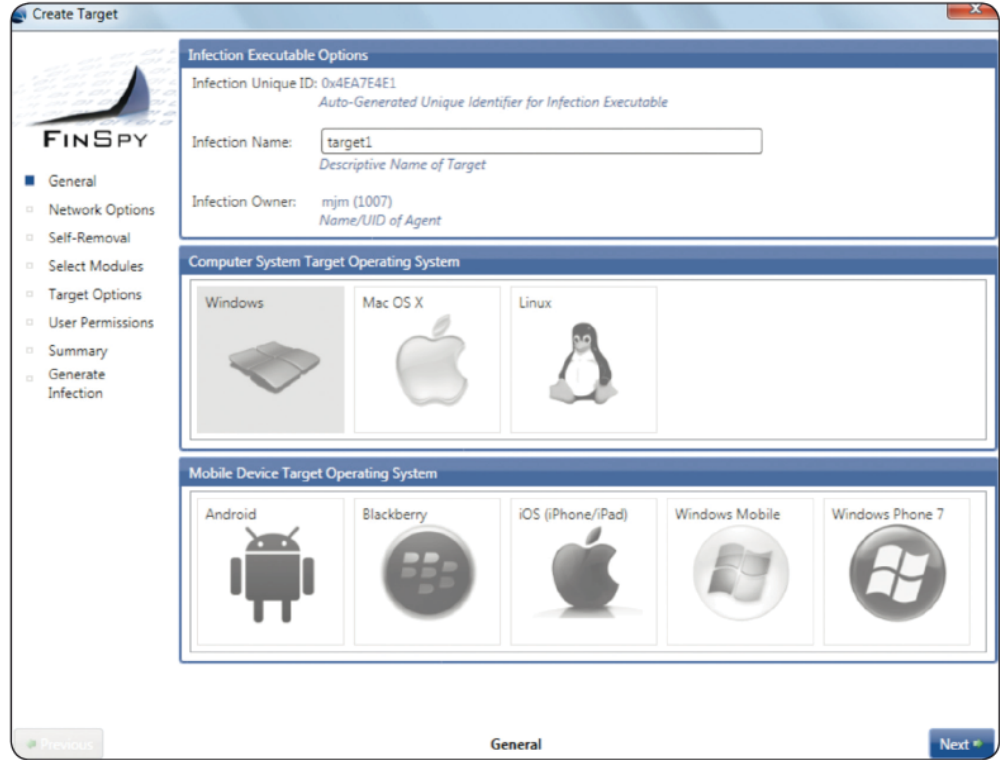
Name	M	T	IMEI	IMSI	Phone Number	OS	Provider	Global IP	Country	City	Base Station	Heartbeat Type
testV50	-	-	3572	262022	+49172	-	Vodafone	-	Germany	--	262/2/9	SMS
Happy	-	-	3568	262021	+49162	-	Vodafone	192.1	Germany	--	262/2/9	TCP
NoMod	-	-	3554	262021	+49162	-	Vodafone	-	Germany	Harlaching	262/2/9	SMS
test3	-	-	3588	262021	+49162	-	Vodafone	77.25	Germany	--	262/2/9	TCP
MalagaX	-	-	3585	262011	+49151	-	T-Mobile	-	Germany	--	262/1/1	SMS
SII	-	-	3584	262011	+49151	-	T-Mobile	-	Germany	Harlaching	262/1/1	SMS
SocketX	-	-	3538	262026	+49152	-	Vodafone	-	Germany	--	262/2/9	SMS
Nexus12	-	-	3549	262022	+49172	-	Vodafone	-	Germany	--	262/2/9	SMS
MalagaX	-	-	1234	666666	-	-	-	-	Unknown	--	12/666	SMS
sony	-	-	1259	262022	+49172	-	Vodafone	-	Unknown	--	-1/-1/0	SMS
testV44	-	-	3523	262011	+49151	-	T-Mobile	-	Germany	--	262/1/1	SMS
GalaTab	-	-	3529	262022	+49172	-	Vodafone	192.1	Germany	Harlaching	262/2/9	TCP
test3	-	-	3526	262021	+49162	-	Vodafone	109.4	Germany	--	262/2/9	TCP



حلول النشر، والمراقبة عن بعد

FINSPY MOBILE

يعمل على المنصات النقالة المعروفة كلها



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

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

info@gammagroup.com

WWW.FINFISHER.COM

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

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 المشككة تلقائياً عند إدخاله إلى الكمبيوتر مع تدخل بسيط من المستخدم أو من دونه، كما أن استخدامه في العمليات لا يتطلب عملاء يتمتعون بخبرة في تكنولوجيا المعلومات. يمكن استخدامه مع أنظمة متعددة قبل إعادته إلى المقر.

مثال الاستخدام ٢: الوكالة الاستخباراتية

تم تزويد مخبر في مجموعة إرهابية محلية بـ FinFly USB لتركيب حل مراقبة عن بعد سراً على أنظمة كمبيوتر 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: وحدة المراقبة التقنية

في بلدان عديدة، تم استخدام FinFly USB من قبل وحدات المراقبة التقنية لتركيب حل المراقبة عن بعد في الأنظمة المستهدفة التي تكون مطفأة وذلك بكل بساطة من خلال تشغيل النظام من جهاز FinFly USB. يمكن تطبيق هذه التقنية حتى على الأنظمة المستهدفة التي لديها تشفير كامل للقرص الصلب مع منتجات مثل برنامج TrueCrypt.

لمحة شاملة على المميزات

- يمكن أن يركب على الأنظمة المطفأة حتى مع تشفير كامل للقرص الصلب (مثلاً، TrueCrypt)
- يقوم بتركيب حل المراقبة عن بعد سراً عند إدخاله إلى النظام المستهدف
- تدخل بسيط/لا تدخل من قبل المستخدم
- يمكن إخفاء الوظيفة 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.



FINFLY USB

عناصر المنتج



الدمج الكامل لـ FinSpy

- التوليد والتفعيل التلقائي من خلال FinSpy Agent



FinFly USB

- جهاز USB
- ينشر حل المراقبة عن بعد عند إدخاله إلى نظام مستهدف
- ينشر حل المراقبة عن بعد أثناء عملية الإقلاع



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

هاتف: ٤١١ ٣٣٢ - ١٢٦٤ - ٤٤٤

فاكس: ٤٢٢ ٣٣٢ - ١٢٦٤ - ٤٤٤

info@gammagroup.com

WWW.FINFISHER.COM

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

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 وعدم فتح المستهدفين أي ملفات أرسلت إلى حساباتهم عبر البريد الإلكتروني.

يعتبر المستهدفون الذين يتمتعون بالتوعية الأمنية بشكل خاص هدفاً تستحيل مراقبته بما أنهم يحافظون على حداثة أنظمتهم ولا تنجح معهم أي أعمال برمجيات اختراق أساسية.

تم تصميم FinFly LAN ينشر سراً حل المراقبة عن بعد في الأنظمة المستهدفة في الشبكات المحلية (اللاسلكية واللاسلكية/اللاسلكية/اللاسلكية). هو قادر على إصلاح أخطاء الملفات التي ينزلها المستهدف فوراً أو على إرسال تحديثات مزيفة للبرمجيات الأكثر شيوعاً أو على ضخ الحمولة في المواقع الإلكترونية التي تتم زيارتها.

مثال الاستخدام ٢: مكافحة الفساد

تم استخدام FinFly LAN للقيام 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 بالمواقع الإلكترونية التي كان المستهدف يزورها وذلك لإطلاق عملية التركيب.

مثال الاستخدام ١: وحدة مراقبة تقنية

أمضت وحدة مراقبة تقنية أسابيع تتعقب مستهدفاً من دون أن تتمكن من الولوج جسدياً إلى جهاز الكمبيوتر خاصته. استخدمت هذه الوحدة FinFly LAN لتركيب حل المراقبة عن بعد على النظام 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 اللاسلكية واللاسلكية (٨٠٢,١١)
- يمكن دمجه مع عدة FinIntrusion للولوج سراً إلى الشبكة
- يخفي حل المراقبة عن بعد في تنزيلات المستهدفين
- يبيّن حل المراقبة عن بعد على شكل تحديث للبرمجيات
- يقوم بعادياً، بتركيب حل المراقبة عن بعد من خلال المواقع الإلكترونية التي يزورها المستهدف

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



FINFLY LAN

عناصر المنتج



عدة FinIntrusion – الدمج (اختياري)

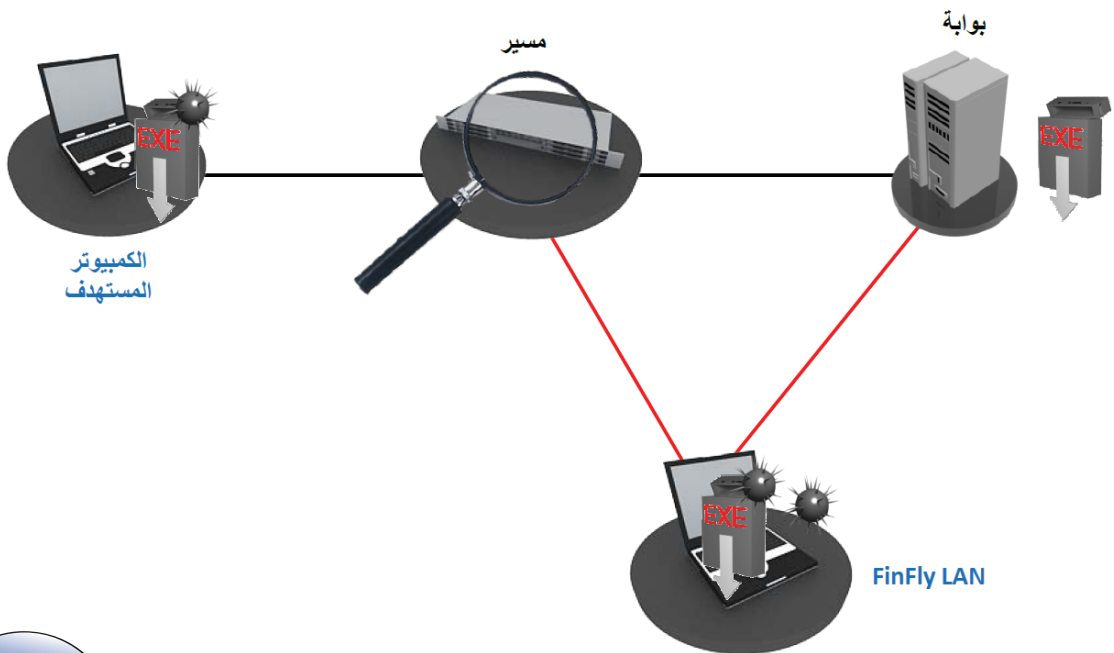
- يمكن إطلاق FinFly LAN كوحدة في عدة FinIntrusion



FinFly LAN

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

النشر من خلال الشبكات المحلية

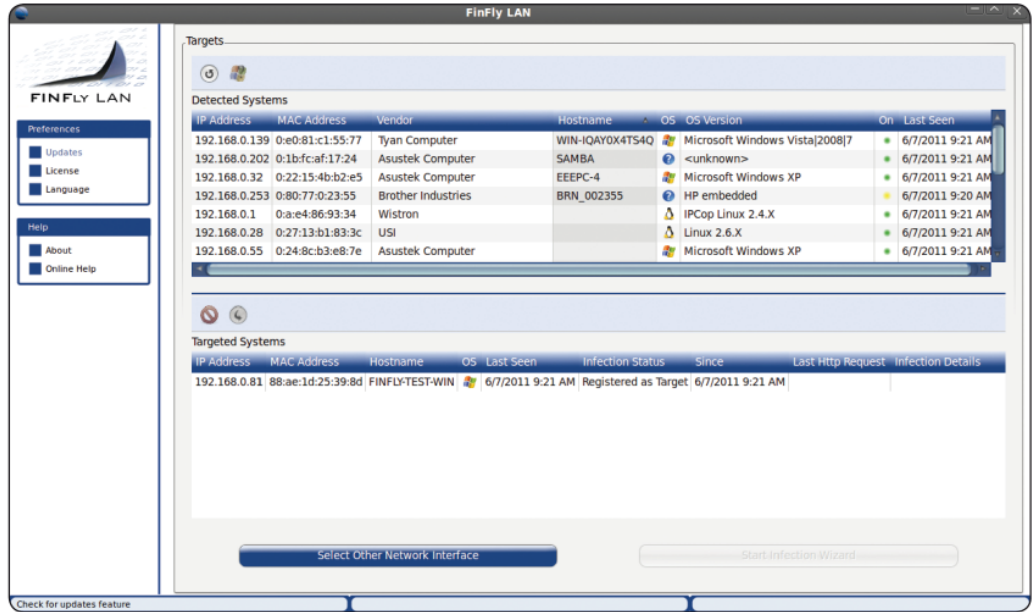


حلول النشر، والمراقبة عن بعد

FINFLY LAN

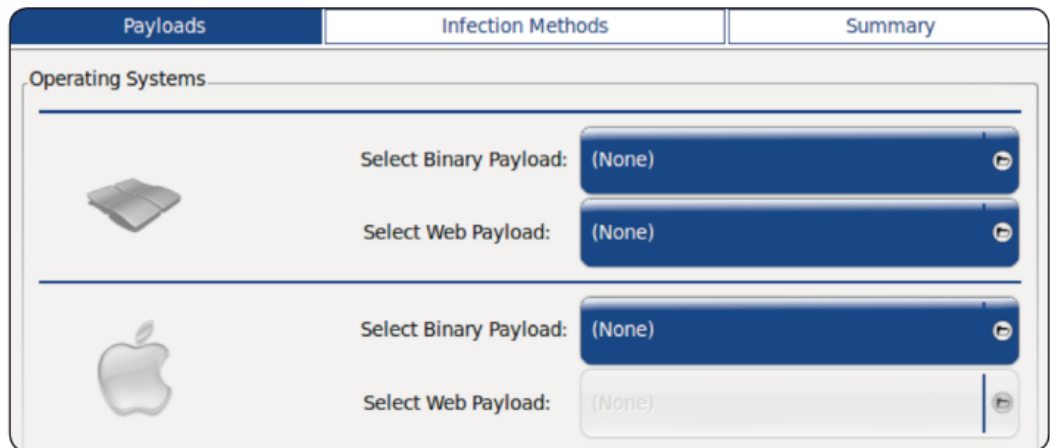
واجهة بينية مؤتمتة

- سهولة الاستخدام من دون تدريب معقد



استيعاب مستهدفين متعددين وملفات قابلة للتنفيذ

- يمكن إضافة ملفات مختلفة قابلة للتنفيذ لكل مستهدف



GAMMA GROUP

GAMMA INTERNATIONAL
المملكة المتحدة

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

info@gammagroup.com

WWW.FINFISHER.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 محذوفة من هذا المستند.

حلول النشر، والمراقبة عن بعد

FINFLY WEB

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

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

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

في FinFly Web واجهة ببنية سهلة الاستخدام «أشُر وانقر» تتيح للعميل تشكيل رمز نشر مكيف وفقاً لوحدة مختارة.

يتم نشر الحمولة عندما يزور النظام المستهدف المواقع الإلكترونية المجهزة بالرمز المكيف.

مثال الاستخدام ٢: وكالة استخباراتية

نشر العميل FinFly ISP لدى المزود الأساسي بخدمة الإنترنت في بلاده، وكان مرفقاً بـ FinFly Web لنشر الحمولة عن بعد، عندما زار المستهدف موقعاً إلكترونياً موثقاً.

مثال الاستخدام ١: وحدة المراقبة التقنية

بعد تحديد مواصفات أحد المستهدفين، أنشأت الوحدة موقعاً إلكترونياً يهيمه 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

- وحدة وب قابلة للتكيف كلياً
- يمكن تركيبه سراً في أي موقع إلكتروني
- اندماج تام مع FinFly LAN و FinFly NET و FinFly ISP ليتم نشره حتى ضمن مواقع إلكترونية مألوفة 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 المشكّلة

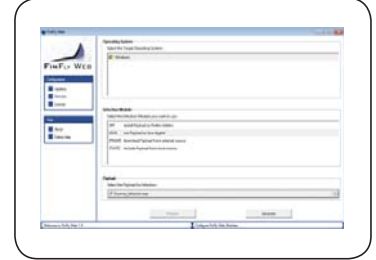
للحصول على المزيد من التفاصيل في ما يتعلق بالمميزات، يرجى مراجعة مميزات المنتج.



حلول النشر، والمراقبة عن بعد

FINFLY WEB

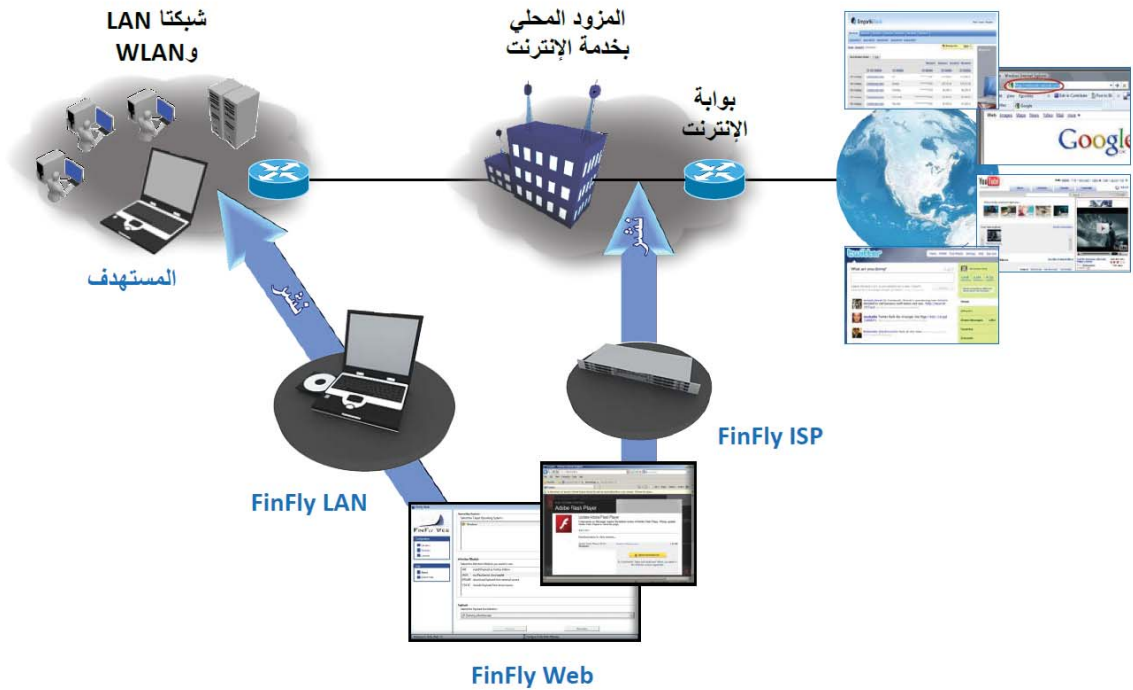
عناصر المنتج



FinFly Web

- صانع مواقع إلكترونية قابل للتكيف

اندماج كامل مع FinFly LAN و FinFly ISP



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

هاتف: ٤١١ ٣٣٢ - ١٢٦٤ - ٤٤٤

فاكس: ٤٢٢ ٣٣٢ - ١٢٦٤ - ٤٤٤

info@gammagroup.com

WWW.FINFISHER.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 محذوفة من هذا المستند.

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

قد لا يكون ممكناً أحياناً تنفيذ أساليب نشر معيارية لحلول المراقبة عن بعد عندما يتعلق الأمر بمستهدفين المتمرسين الذين خضعوا للتدريب المكثف والذين يتمتعون بوعي عميق بما أنهم على وعي بتقنيات وأدوات النشر الشائعة.

في العديد من السيناريوهات، تتيح هجمات يوم الصفر أسلوباً قوياً وموثوقاً لنشر حلول المراقبة عن بعد وذلك من خلال استكشاف نقاط الضعف في البرمجيات التي يستخدمها المستهدف.

يتيح FinFly Exploit Portal الولوج إلى مجموعة واسعة من هجمات يوم الصفر أو اليوم واحد للبرمجيات الشائعة مثل **Microsoft Office، Internet Explorer، Adobe Acrobat Reader** وسواها.

مثال الاستخدام ٢: وكالة استخباراتية

تم تحديد الهدف في زاوية نقاش ولكن لم يتح الاتصال المباشر أو بواسطة البريد الإلكتروني. أنشأت الوكالة خادم شبكة يحوي هجمات يوم الصفر على **Internet Explorer**، قام بنشر الحمولة في النظام المستهدف عندما فتح المستهدف URL الذي أرسل إليه من خلال رسالة خاصة في زاوية النقاش.

مثال الاستخدام ١: مجموعة إجرامية تعتمد تكنولوجيا عالية الجودة

كانت إحدى المجموعات الإجرامية تحقق في إحدى جرائم الإنترنت واحتاجت إلى نشر حل مراقبة عن بعد على أحد الأنظمة المستهدفة. فاستخدمت هجمة يوم الصفر على برنامج **Adobe Acrobat Reader** وأرسلت ملف PDF عبر البريد الإلكتروني إلى المستهدف. انتشر حل المراقبة عن بعد تلقائياً عندما فتح المستهدف الملف.

لمحة شاملة على المميزات

- ولوج تام إلى بوابة الإنترنت وإلى **Exploit Generator**
- هجمات يوم الصفر للمستوى الحكومي، تنفذ بواسطة أنظمة متعددة
- مستويات تصحيح الأخطاء من دون تعديلات إضافية
- ٤ هجمات كبيرة على الأقل (برمجيات شائعة متصفح/بريد/File Viewer)
- متوفر على الدوام
- ضمانة لمدة ٣٠ يوماً لكل هجمة ضمن البوابة
- يحدث باستمرار هجمات اليوم الواحد لبرمجيات متعددة

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



عناصر المنتج



بوابة Finfly Exploit

- مكتبة Exploit على واجهة الوب

نموذج لبوابة FinFly Exploit

■ Microsoft Internet Explorer 9-8-7-6 Remote Code Execution Exploit

A use-after-free vulnerability exists in Microsoft Internet Explorer when processing certain JavaScript and HTML data, which could be exploited to compromise a vulnerable system via a specially crafted web page.

The vulnerability affects Microsoft Internet Explorer 9, 8, 7 and 6, on Windows 7 SP1 and prior, Windows Vista SP2 and prior, and Windows XP SP3 and prior.

The provided code execution exploit bypasses ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention) and works on all Windows systems.

• [More Information and Details](#) (Exploit updated on 2011-10-14. Exploit first released on 2011-08-06)

■ Microsoft Internet Explorer 9-8 Remote Sandbox Bypass Exploit

A vulnerability exists in Microsoft Internet Explorer's sandbox (Protected Mode) when processing certain data from a Low integrity process, which could be exploited to achieve code execution at Medium integrity and bypass Protected Mode.

The vulnerability affects Microsoft Internet Explorer 9 and 8 on Windows 7 SP1 and prior and Windows Vista SP2 and prior (Windows XP SP3 and prior do not include a sandbox).

The provided exploit must be combined to another IE code and must be used as a second stage shellcode.

• [More Information and Details](#) (Exploit updated on 2011-10-14. Exploit first released on 2011-03-02)

■ Adobe Acrobat & Reader 9.x PDF Processing Code Execution Exploit

A buffer overflow vulnerability exists in Adobe Acrobat and Reader when processing certain data within a PDF document, which could be exploited to compromise a vulnerable system by tricking a user into opening a malicious PDF file.

The provided code execution exploit bypasses ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention) and works on all Windows systems.

• [More Information and Details](#) (Exploit updated on 2011-09-02. Exploit first released on 2011-07-15)



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

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

info@gammagroup.com

WWW.FINFISHER.COM

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

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

مثال الاستخدام: وكالة استخباراتية

تم نشر FinFly ISP في شبكات المزود الأساسي بخدمة الإنترنت في البلاد وقد تم استخدامه لنشر حل المراقبة عن بعد على الأنظمة المستهدفة. وطالما أن المستهدفين الموصولين 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 المراقبة عن بعد وسراً، من أجل التمكن من مراقبة الهدف من المقر.

FinFly ISP هو حل استراتيجي يمتد داخل البلاد وتكتيكي (نقال) يمكن دمجه في مدخل مزود خدمة الإنترنت و/أو الشبكة المركزية للتمكن من تركيب حل المراقبة عن بعد، بعادياً على الأنظمة المستهدفة المختارة.

ترتكز أدوات FinFly ISP على تكنولوجيا خادم موثوقة ذات قدرات هائلة يعتمد عليها لمواجهة أي تحدٍ مرتبط بطوبولوجيا الشبكة. مجموعة كبيرة من الواجهات البيئية 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 التواصل التفاعلي بين FinFly ISP وخوادم AAA- تؤكد بأنه قد تم تحديد المستهدفين وبأن تبادلاتهم قابلة للنشر.

FinFly ISP قادر على إصلاح الأخطاء في الملفات التي يتم تنزيلها من قبل المستهدف على الفور أو إرسال تحديثات مزيفة للبرمجيات من برمجيات شائعة. ويشمل الإصدار الجديد تطبيق FinFly Web وهو تطبيق النشر عن بعد من Gamma الذي يضح حمولة في أي موقع إلكتروني يزوره المستهدف.

لمحة شاملة عن المميزات

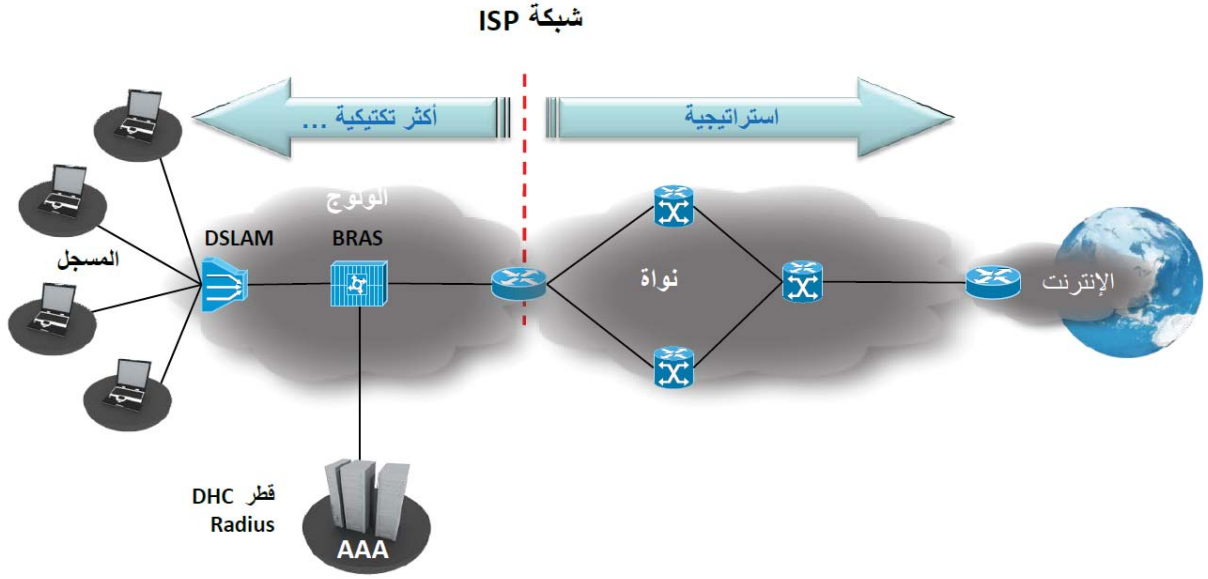
- يمكن تركيبه داخل شبكات المزود بخدمة الإنترنت
- يستوعب البروتوكولات الشائعة كافة
- يختار المستهدفين وفقاً لعنوان بروتوكول الإنترنت واسم الولوج Radius وDHCP وMSISDN.
- يخفي حل المراقبة عن بعد في تنزيلات المستهدفين
- يبيّن حل المراقبة عن بعد على شكل تحديث للبرمجيات
- يقوم بعادياً، بتركيب حل المراقبة عن بعد من خلال المواقع الإلكترونية التي يزورها المستهدف

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



المواقع 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 الأهداف ونشر الحمولة من المقر البعيد من دون الحاجة إلى أن تكون الوكالة الموكلة تطبيق القانون في الموقع.

بالطبع يمكن دمج الحلول التكتيكية والاستراتيجية معاً لاستمثال مرونة عمليات النشر.

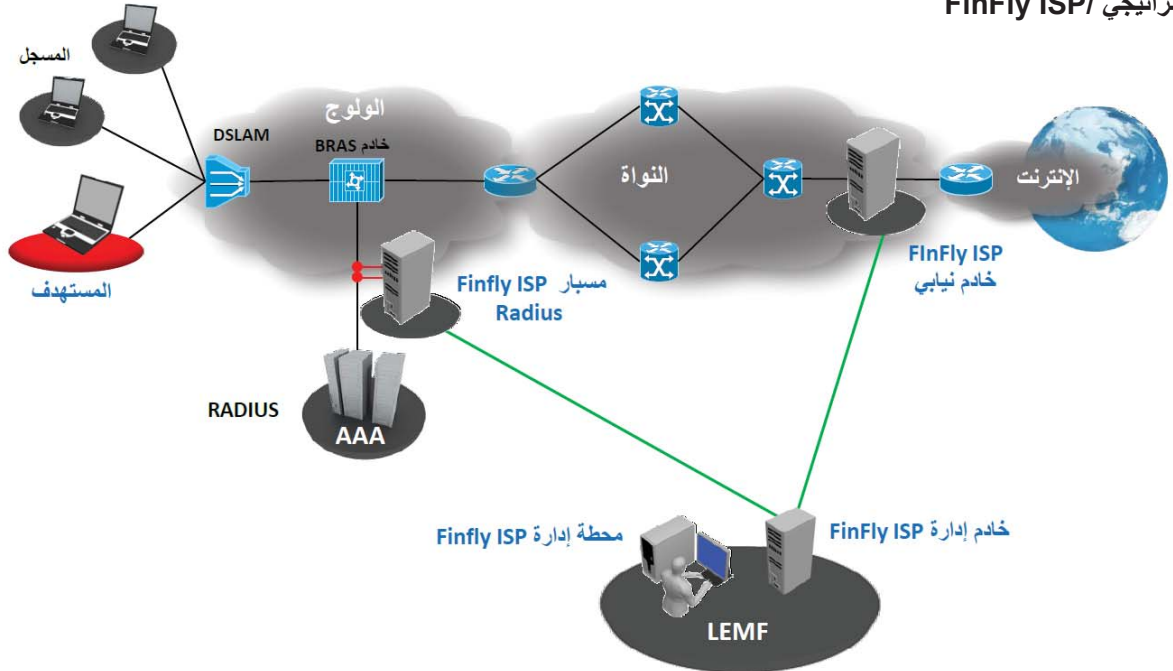
إن هذا الحل التكتيكي نقال والتجهيزات مخصصة لمهام النشر داخل شبكة الوصول القريبة من نقاط وصول المستهدف. يمكن نشر هذا الحل على المدى القصير لتوفير المتطلبات التكتيكية المرتكزة على مستهدف معين أو على مجموعة صغيرة من المستهدفين في منطقة ما.



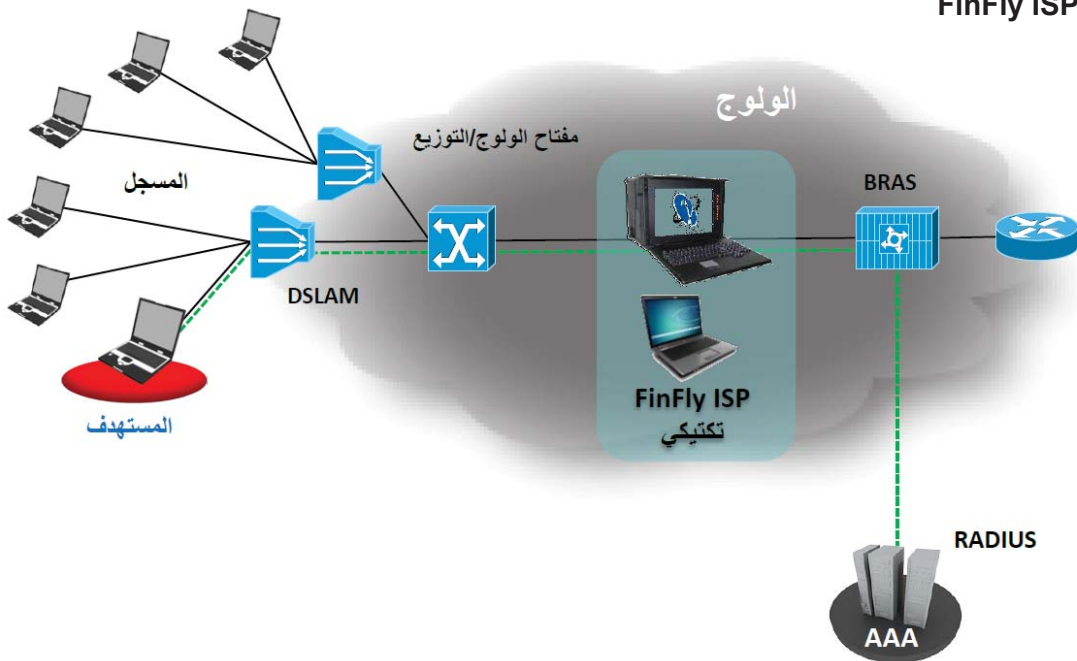
FINFLY ISP

تشكيل الشبكة

FinFly ISP/ ستراتيجي



FinFly ISP/ تكتيكي



حلول النشر، والمراقبة عن بعد

FINFLY ISP

الإنتاجية:	< ٢٠ جيجابايت في الثانية
العدد الأقصى لبطاقات واجهة الشبكة:	٨ - ٢
الواجهات البينية:	١ GE نحاس/ ألياف ١٠ GE نحاس/ ألياف SONET/SDH OC ٣-١٩٢ STM-١/٦٤ ATM AAL٥
أجهزة المعالجة:	٨ - ١٠ Intel XEON معالج ثنائي النواة أو ثماني النواة
ذاكرة الوصول العشوائي:	١٢ جيجابايت - ١ تيرابايت
سعة القرص الصلب:	١٤٦x٣ جيجابايت - ٤,٨TB SAS
المزايا:	٣ HP iLO طاقة زائدة مراوح وظيفة تحويل التجاوز (في حال كان ذلك ممكناً)
نظام التشغيل:	Linux GNU (Debian 5.0) معزز

الإنتاجية:	٦ جيجابايت في الثانية
العدد الأقصى لبطاقات واجهة الشبكة:	٣
الواجهات البينية:	1x1000BASE-T (نحاس؛ منفذان) 1x1000BASE-SX (الألياف؛ منفذان) 1x1000BASE-LX (الألياف؛ منفذان) واجهات أخرى عند الطلب
أجهزة المعالجة:	١ Intel Core i٧ Intel Xeon عند الطلب
النواة:	معالج رباعي النواة
ذاكرة الوصول العشوائي:	١٢ جيجابايت كحد أدنى
سعة القرص الصلب:	١x٢ تيرابايت SATA
محرك القرص الضوئي:	DVD+/-RW SATA
المراقبة:	١٧ x١ بوصة TFT ، لوحة مفاتيح، لوحة لمسية
المزايا:	وظيفة تحويل التجاوز لبطاقات واجهة الشبكة
نظام التشغيل:	Linux GNU (Debian 5.0) Windows ٧ Prof. (Management Nb.)

عناصر المنتج

جهاز FinFly ISP الاستراتيجي

يتطلب نشر FinFly ISP الاستراتيجي ما يلي:

- نظام الإدارة في الوكالات الموكلة تطبيق القانون
- خادم (خوادم) تحديد المستهدف في نظام AAA على الشبكة
- خادم (خوادم) نيابي للنشر في بوابة (بوابات) الإنترنت مثلاً.



جهاز FinFly ISP التكتيكي

يتألف نظام FinFly ISP التكتيكي ما يلي:

- خادم نيابي نقال للنشر وتحديد المستهدفين
- حاسوب نظام الإدارة



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

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

info@gammagroup.com

WWW.FINFISHER.COM

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

حلول النشر، والمراقبة عن بعد

FINFLY NET

معلومات سريعة	
الاستخدام:	• عمليات تكتيكية
القدرات:	• نشر حل المراقبة عن بعد في النظام المستهدف في بيئة شبكة محلية «صديقة».
المحتوى:	• برمجيات/تجهيزات

مثال الاستخدام: وكالة استخباراتية

يتم نشر FinFly NET على الشبكة المحلية لأحد الفنادق في مقدمة مودم DSL قبل بدء المبادلات مع شبكة مزود بالخدمة.

يتم تحديد المستهدفين في المبادلات من خلال وسائل سلبية لتحديد مواصفاتهم وتعيينهم ويتم نشر حل المراقبة عن بعد على الأنظمة المستهدفة المطلوبة بحسب عملية التحديد.

في العديد من العمليات الواقعية، لا يمكن الوصول جسدياً إلى الأنظمة المستهدفة داخل البلاد.

ولحل هذه المسألة يجب تركيب حل مراقبة عن بعد بشكل سري وبعادياً ، من أجل التمكن من مراقبة الهدف من المقر.

يقوم FinFly NET على كمبيوتر محمول عالي الكفاءة مدمج مع كمبيوتر محمول للإدارة ليسهل نقله ومرونة استعماله في الشبكات المستهدفة. مجموعة واسعة من بطاقات واجهة الشبكة- وكلها محمية بوظائف تجاوز- متوفرة للاتصال النشط بالشبكة.

يمكن للمستخدم النهائي أن يختار وسائل سلبية متقدمة ومختلفة لتحديد المستهدف والمبادلات. وتتراوح هذه الوسائل بين مراقبة DHCP/ RADIUS (عناوين MAC وأسماء المستخدمين) ومراقبة التدفق وبصمات الأصابع. يمكن أن تستخدم كل من الوسائل كوسيلة مستقلة كما يمكن أن تدمج مع وسائل أخرى وذلك من أجل إتاحة تحديد المستهدفين قدر الإمكان. من المؤكد أنه يمكن استخدام عناوين بروتوكول الإنترنت الثابتة أيضاً.

هو قادر على إصلاح أخطاء الملفات التي ينزلها المستهدف فوراً أو على إرسال تحديثات مزيفة للبرمجيات الأكثر شيوعاً أو على ضخ الحمولة في المواقع الإلكترونية التي تتم زيارتها.

لمحة شاملة عن المميزات

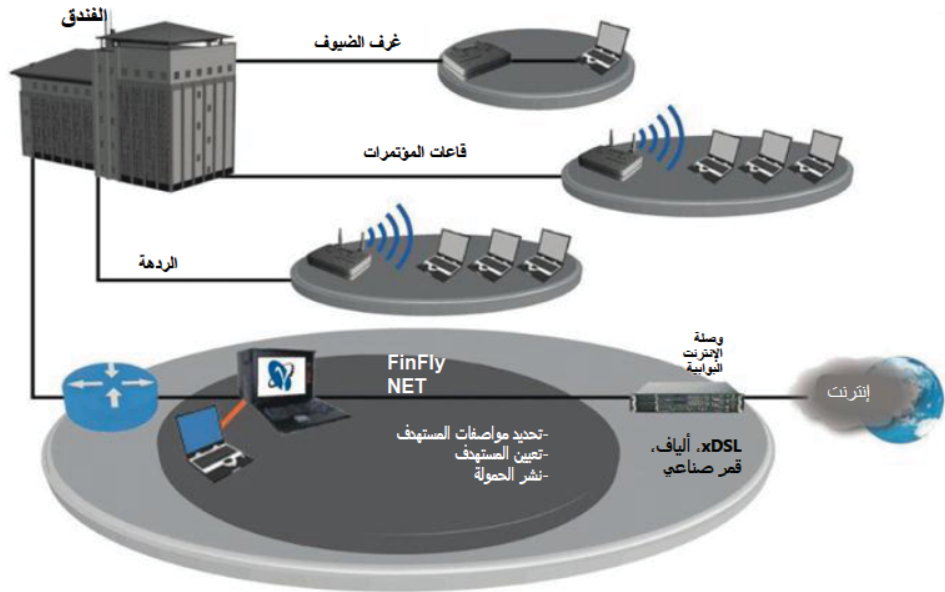
- يمكن تركيبه في بيئة شبكة محلية (فندق، نقطة ساخنة، مؤسسة...)
- إيترنت Base-T، Base-SX، Base-LX، Base-LX
- يحدد المستهدفين بواسطة طرق سلبية لتحديد مواصفاتهم/تعيينهم
- يخفي حل المراقبة عن بعد في تنزيلات المستهدفين
- يضخ حل المراقبة عن بعد على شكل تحديث للبرمجيات
- يركب حل المراقبة عن بعد من خلال المواقع الإلكترونية التي يزورها المستهدف

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

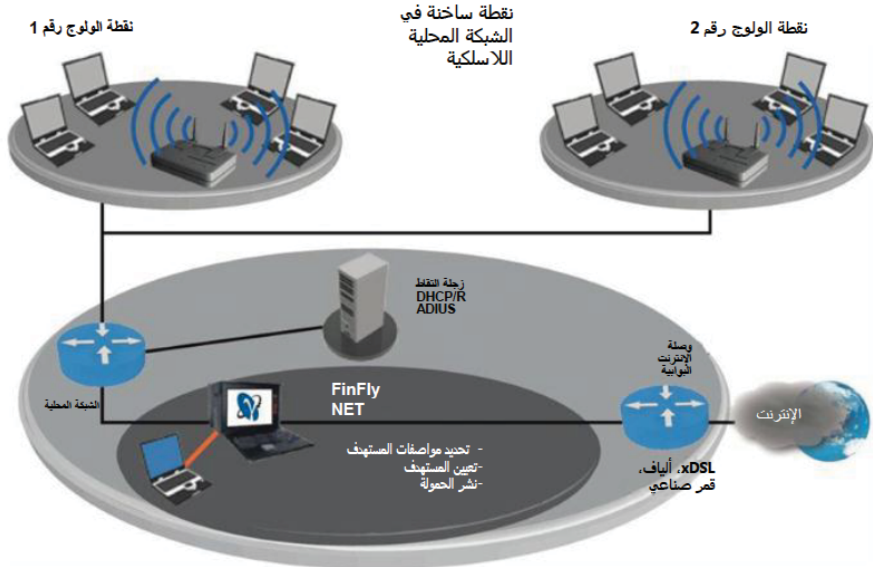


إمكانية نشر مختلفة

النشر في الشبكة المحلية لأحد الفنادق



النشر في الشبكة المحلية لنقطة ساخنة في الشبكة المحلية اللاسلكية



سيتم نشر FinFly NET في الموقع المناسب داخل المنشأة. وبعد وصل الكمبيوتر النقال إلى الوصلة (الوصلات) الموقرة. يمكن للمستخدم أن يبدأ بتحليل المبادلات مختاراً وسائل عديدة من أجل تحديد المستهدفين ومبادلاتهم. وتعتمد الوسائل التي يجب استخدامها لتحديد المستهدفين على إعدادات الشبكة وميزاتها والخدمات المقدمة والمستخدم.



تحديد مواصفات المستهدفين وتعيينهم

وحدة التقاط بروتوكول النص الفائق
أنواع وإصدارات المتصفحات وأنظمة التشغيل والتاريخ واللغات

وحدة التقاط البريد الإلكتروني
SMTP, POP3

وحدة التقاط كلمة الدخول
FTP, HTTP, IMAP, IRC, NNTP, POP, SMTP

وحدة التقاط TCP/UDP
بروتوكول الإنترنت للمصدر/المقصد. منافذ المصدر/المقصد

وحدة التقاط DHCP/RADIUS
MAC. اسم المضيف. بداية/نهاية جلسة IP

وسائل النشر لدى المستهدفين

ثنائي/تنزيل
تصبح أخطاء ملفات "exe." و/أو "scr."

ضخ التحديثات
تحديثات مزورة لتطبيقات مختلفة

النشر في المواقع الإلكترونية
باستخدام FinFly Web للنشر في خلال عملية التصفح



حلول النشر، والمراقبة عن بعد

FINFLY NET

عناصر المنتج

الإنتاجية:	٦ جيجابايت في الثانية
العدد الأقصى لبطاقات واجهة الشبكة:	٣
الواجهات البينية:	1x1000BASE-T (نحاس؛ منفذان) 1x1000BASE-SX (ألياف-MM؛ منفذان) 1x1000BASE-LX (ألياف-SM؛ منفذان) واجهات أخرى عند الطلب
أجهزة المعالجة:	١ × Intel Core i Intel Xeon عند الطلب
النواة:	رباعي النواة/رباعي
ذاكرة الوصول العشوائي:	١٢ جيجابايت كحد أدنى
سعة القرص الصلب:	١ × ٢ تيرابايت SATA
محرك القرص الضوئي:	DVD+/-RW SATA
المراقبة:	١٧ × ١ بوصة TFT ، لوحة مفاتيح، لوحة لمسية
المزايا:	وظيفة تحويل التجاوز لبطاقات واجهة الشبكة
نظام التشغيل:	معزز Linux GNU (Debian 5.0) Windows Prof. (Management Nb.)

يشمل FinFly NET ما يلي:

- خادم نيابي لتحديد مواصفات المستهدف وتعيينه وللنشر (نقال)
- نظام إدارة (كمبيوتر محمول)



ملاحظة مهمة:

توفر Gamma إلى جانب FinFly NET القدرات الاستخباراتية نفسها التي يوفرها حل FinSpy ISP، حيث تدخل قدرات تحديد المستهدفين في إطار حل ISP ثابت أو نقال. يتميز هذا الحل بخادم ذي تكنولوجيا رفيعة الأداء يتم تكييفها وإدماجها في بيئة ISP وبالشروط ذات الصلة.



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

هاتف: ٤١١ ٣٣٢ - ١٢٦٤ - ٤٤٤

فاكس: ٤٢٢ ٣٣٢ - ١٢٦٤ - ٤٤٤

info@gammagroup.com

WWW.FINFISHER.COM

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

FINTRAINING

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



برنامج التدريب على اختراق تكنولوجيا المعلومات

FINTRAINING

معلومات سريعة	
• تبادل المعرفة	الاستخدام:
• الدراية في مجال اختراق تكنولوجيا المعلومات • قدرات لمواجهة حرب الإنترنت	القدرات:
• تدريب	المحتوى:

تقوم **Gamma** بتحويل حصص التدريب الفردية 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.

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

من جهة أخرى، إن مواضيع مثل حرب الإنترنت 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 يتعين على المستخدم النهائي أن يقوم به للتمكن من مواجهة التحديات اليومية التي تعترضه.

برنامج استشارات

- برنامج كامل للاستشارات والتدريب على اختراق تكنولوجيا المعلومات
- تشكيل وتدريب منظم لفريق عمل اختراق تكنولوجيا المعلومات
- تقييم كامل لأعضاء الفريق

أمثلة عن مواضيع حصص التدريب

- تحديد مواصفات المواقع الإلكترونية المستهدفة والأشخاص المستهدفين.
- تعقب البريد الإلكتروني المجهول
- ولوج عن بعد إلى حسابات البريد الإلكتروني
- تقييم أمن خوادم الويب وخدمات الويب
- استغلال البرمجيات عملياً
- اختراق تكنولوجيا المعلومات لاسلكياً (الشبكة اللاسلكية/ 802.11 والبلوتوث)
- هجمات على البنى التحتية الأساسية
- سلب البيانات واعتمادات المستخدم على الشبكات
- مراقبة نقاط الاتصال اللاسلكي ومقاهي الإنترنت وشبكات الفنادق.
- اعتراض الاتصالات وتسجيلها (بروتوكول الصوت عبر الإنترنت (VoIP و DECT)
- استعادة كلمات المرور



برنامج التدريب على اختراق تكنولوجيا المعلومات

FINTRAINING

دورات تدريبية مكيفة في منشآت تدريب حديثة حول العالم



GAMMAGROUP

GAMMA INTERNATIONAL
المملكة المتحدة

هاتف: ٤١١ ٣٣٢ - ١٢٦٤ - ٤٤٤

فاكس: ٤٢٢ ٣٣٢ - ١٢٦٤ - ٤٤٤

info@gammagroup.com

WWW.FINFISHER.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 محذوفة من هذا المستند.

دعم منتجات FINFISHER

FINSUPPORT

معلومات سريعة

• حل كامل ودعم تشغيلي	الاستخدام:
• تصحيح الأخطاء وتحديث المميزات والقدرات	القدرات:
• برمجيات/تجهيزات	المحتوى:

تحديثات البرمجيات

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

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

FinSupport

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

FinLifeLineSupport

يقدم FinLifeLineSupport دعماً مهنياً للمكتب الخلفي لحل المشاكل والاستفسارات التقنية. كذلك يوفر دعماً للمكتب الخلفي عن بعد تصحيح أخطاء FinFisher™ SW واستبدال التجهيزات بموجب كفالة.

بالإضافة إلى ذلك، يحصل الزبون تلقائياً على المميزات والوظائف الجديدة مع وظيفة تصحيح الأخطاء.





GAMMAGROUP

GAMMA INTERNATIONAL

المملكة المتحدة

هاتف: ٤١١ ٣٣٢ - ١٢٦٤ - ٤٤٤

فاكس: ٤٢٢ ٣٣٢ - ١٢٦٤ - ٤٤٤

info@gammagroup.com

WWW.FINFISHER.COM

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