WHITE PAPER

MANDIANT®
A FireEye® Company

Proactive Cyber Investigations

A model approach

FireEye®

Introduction

Cyber crime[1] is a pervasive global issue that continues to grow in scale and complexity. Governmental organisations and law enforcement agencies (LEAs) around the world typically identify cyber crime as a systemic threat.[2, 3] Despite progress on the defensive front, including initiatives such as the **Directive on the Security of Networks and Information Systems**, there has been little progress in developing an effective approach to investigate cyber crime, when judged by the capacity to prosecute — or otherwise disrupt and deter — cyber criminals. This paper sets out a proposed approach for effective cyber crime investigation.

There are several barriers to the effective conduct of investigations into cyber crime, including:

The international nature of most cyber attacks. Criminals targeting victims within the borders of a single country will often do so through infrastructure located abroad. Existing legal frameworks and international arrangements for dealing with the collection of evidence (or intelligence) to pursue investigations into cyber attacks are inadequate.

Operational issues around the capacity and capability of LEAs to conduct effective cyber crime investigations, even when empowered to do so. This includes the knowledge and training of staff, the availability of appropriate tools and techniques and the framework to act in a timely fashion.

The extreme pace of cyber crime and general online activity is at odds with the methodical approach of traditional law enforcement procedures, and the development of legislation which underpins these procedures.

Many entities, including the European Commission, acknowledge this capability deficit:

> "**A more effective law enforcement response focusing on detection, traceability and prosecution of cyber criminals is central to building effective deterrence...** In order to increase our chances of bringing perpetrators to justice, we need to urgently improve our capacity to identify those responsible for cyber-attacks"[4]

The frameworks that enable investigations into online crime must change. The digital world has revolutionised the way we live, and this shift has been quickly embraced by criminals. Statistics show that online crime constitutes between one third and one half of all crime in some EU countries, that only 14% of incidents of fraud and computer misuse come to the attention of the police or are reported by the victim, less than 10% of reported cyber crimes are investigated and only around 10% of investigated cases are resolved with a successful outcome.[5, 6, 7] Cyber attacks are typically stacked in the attacker's favour. The actual situation is likely to be worse, with many more cyber crimes never being reported. Tinkering with existing laws or procedures is not enough to deal with radical, fast-paced change.

1 This paper focuses on the operational response to cyber crime through active investigations. As such, cyber crime is defined as any crime which relies primarily, or significantly, on online activity to commit the offence, and where the only viable initial lead to the offender is through online investigation.
2 National Crime Agency (2018). National Strategic Assessment of Serious and Organised Crime.
3 National Crime Agency (2018). Annual Plan, 2018-19: Leading the fight to cut serious and organised crime.
4 European Commission (September 13, 2017). Resilience, Deterrence and Defense: Building Strong Cybersecurity for the EU.
5 Office for National Statistics (July 19, 2018). Crime in England and Wales: year ending March 2018.
6 Her Majesty's Chief Inspector of Constabulary (2017). State of Policing: The annual Assessment of Policing in England and Wales 2016.
7 The Home Office (July 2018). Crime outcomes in England and Wales: Year ending March 2018.

Law enforcement agencies must be properly equipped to effectively investigate cyber crime. To enable proactive investigations, significant changes are required in these areas:

Operational Capability	Authority to Act	Public-Private Cooperation
LEAs need the human skills and technical resources to conduct fast-paced investigations into digital crime. This means significant investment in training and tools. As argued by HMIC in the UK, "Treating [digital] crime as 'specialist' or requiring expertise that is provided only by the few is outdated, inappropriate, and wrong."[8, 9]	LEAs need to be able to follow the trail of evidence as they would with a traditional crime – from the victim machine(s) to the attacker's own infrastructure, through as many intermediate locations as necessary. However, this trail will almost certainly lead to systems overseas and it will be highly perishable. LEAs need a framework that allows them to "pursue" criminals without the delays incurred by arrangements such as current Mutual Legal Assistance Treaties (MLATs). Such authorisation will need to happen locally and will likely require enabling legislation.	For several years, this has been a dominant theme in discussions on tackling cyber crime and two of the more critical areas are LEA visibility and the significant advantage of investigating a "crime in progress." Private sector organisations, whether actual victims of cyber crime or the cyber incident response (CIR) companies that investigate crimes, have the potential to provide LEAs with active leads. Combining these leads with the appropriate authority to act provides the best opportunity to track, identify and disrupt cyber criminals.

If implemented together, the above measures provide a roadmap to create properly skilled and resourced LEAs that are empowered to effectively investigate cyber crime and ultimately, prosecute or disrupt the attackers responsible. Under this model, LEAs would work closely with the private sector to:

Identify attacks of interest	Launch an active investigation with the objective of identifying the attacker responsible	Deploy appropriate tools to track and identify the attacker	Bring a prosecution or implement other effective disruption or deterrent measures

This approach should provide the foundation for the large-scale investigation of cyber crime and operate alongside more strategic initiatives such as botnet takedowns.

When LEAs use a proactive approach to exploit opportunities to actively track cyber attackers anywhere, we can address the huge global volume of cyber crime.

8 Her Majesty's Chief Inspector of Constabulary (February 2016). State of Policing: The Annual Assessment of Policing in England and Wales 2015.
9 Her Majesty's Chief Inspector of Constabulary (December 2015). Real lives, real crimes: A study of digital crime and policing.

"In the digital world our ability to apply technology quickly will…shape our operational effectiveness, which will in turn influence the level of relevance we have to an increasingly online public. We will be judged accordingly."[10]

— Chief Constable Stephen Kavanagh, Lead for Digital Investigation and Intelligence (DII)

Pro-Active Cyber Investigation Model (PACIM)

Cyber crime is a complex topic and covers myriad offences. Still, the principles of investigation are the same as for traditional crime: the police must begin with a victim or reported crime, and attempt to gather a trail of evidence which will ultimately lead to the perpetrator. Identifying the perpetrator is not the end of the investigation process, but it is the first phase: building the prosecution case, gathering more targeted evidence or intelligence focused on the attacker, or identifying other crimes in progress can only occur after the perpetrator is identified.

Available statistics indicate that most cyber crime is not actively investigated, with a tiny fraction moving to prosecution or conviction. Several elements are required to address this policing void and create an effective model for LEA cyber investigations. An appropriate model will enable LEA to go beyond the current limited, reactive approach and take advantage of public-private cooperation and other opportunities to investigate and proactively track down cyber criminals. Such a model would operate alongside more focused strategic initiatives, such as botnet takedowns or dark market disruptions.

A proactive model for cyber investigations will require changes in operational capability, authority to act and public-private cooperation.

Operational Capability

Training

The capacity to investigate cyber crime often begins with training — all LEA officers should be familiar with attacker methodologies (tactics, techniques and procedures, or TTPs) to understand how to manage online investigations. This is already underway on a limited basis in some country programmes such as the **Digital Investigation and Intelligence Programme in the UK**. However, in the digital age, responsiveness needs to be measured in minutes, hours, or days rather than weeks or months. Basic training must be implemented quickly to give all officers an awareness of the key principles of investigating cyber crime and equip them to respond appropriately.

Most officers will not need specialist training in digital forensics or technical cyber incident response. However, they will need to be able to apply the investigative process in the digital world. All officers and appropriate civilian support staff should understand cyber crime well enough to:

- Gather accurate and relevant information (such as email header information) when receiving crime reports
- Grasp opportunities to gather further material (even if collected by a specialist team)
- Provide basic guidance about the preservation and collection of evidence (for example, when it is best not to power off a computer)
- Prioritise a case based on the information provided

10 PA Consulting Group (April 2015). Digital Investigation and Intelligence: Policing Capabilities for a Digital Age.

This basic cyber awareness training should take 2-3 days as part of starter courses. North Wales Police already runs a one-day cyber crime course for all new Initial Police Learning and Development Programme (IPLDP) recruits.[11] Because cyber crime is so prevalent, general awareness is a skill all officers should have. Increased awareness would also help address a current perceived unease that many officers have with cyber crime, which is a potential barrier to initiating investigations.

Specialist teams, built around existing digital forensics and cyber crime teams, must still maintain the technical capability and expertise needed to collect digital evidence and conduct more complex investigations. These teams will need to monitor the threat landscape and supplement knowledge and capability.

Tools

Tools could be developed in order to facilitate effective investigations into cyber crime. Tracking and identifying perpetrators would be the key objective for tool development: such tools, deployed in a tactical context, can be generically labelled "profilers". Profilers could help address key challenges faced by LEAs, such as attacker operational security measures, including the use of proxies and secure apps. Such tools would require authorisation for deployment based on the well established principles of necessity and proportionality — elements of the Authority to Act.

A profiler is a small piece of software that can be used by LEAs to help trace and identify an attacker. Cyber crime is unusual in that most cases tend to constitute a "crime in progress," either due to ongoing attacker interaction with the initial victim, or due to the attack being high volume in nature, presenting multiple active crime scenes. This characteristic provides the opportunity for LEAs to "pursue" attackers through the deployment of profilers. For instance, in the case of an attacker using information-stealing malware on a system, the profiler could be placed on the victim machine for the attacker to remove.

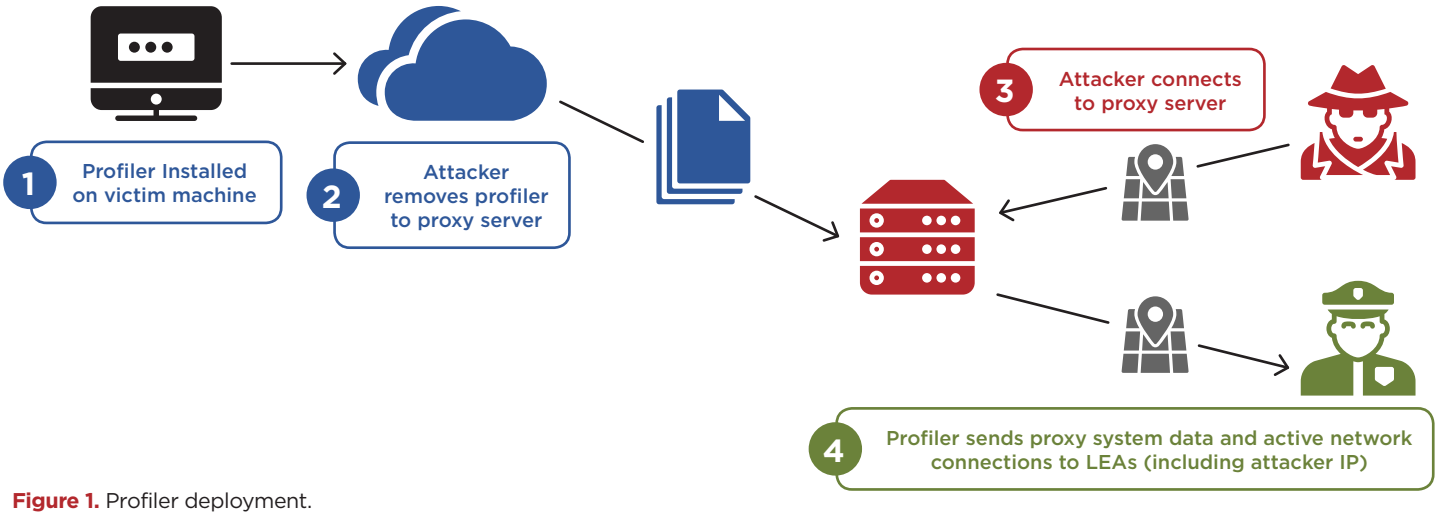

Figure 1. Profiler deployment.

11 Parliament Street (March 20, 2018). Policing and Cybercrime.

Where LEAs have proper and appropriate authorisation for deploying tools, profiler functionality should at least include fingerprinting the host system (hardware, public IP address, OS, etc.) and enumerating active network connections (to help circumvent attacker use of proxy machines), providing the capacity to track attackers even when they are using anonymising proxies. Recent research indicates that many cyber criminals deploy limited operational security measures to mask their origin.[12]

Profilers can be developed as semi-disposable tools, rather than the high end implants associated with significant cost and other barriers to entry. In this sense, we can learn from the attackers — existing code can be tweaked with minimal resources to avoid detection, whilst continuing to function as intended. As such, profiler tools could be deployed swiftly and at scale by LEAs, maintained locally with minimal resource, and without significant impact on budget.

If LEAs, after evaluating the potential risks and consequences, decide to deploy such tools, deployment of a profiler would require training for the officers responsible to ensure an effective operational methodology. Social engineering would be a key element of successful deployment: interacting with a hacker and engineering a situation where the tool is extracted would avoid the need for expensive and scarce exploits, but could, if implemented expertly, also be a highly effective and repeatable methodology. Over time, such social engineering skills should become a standard part of the policing skills framework for cyber investigators and the procedure could be as standard as interviewing suspects during a real-world crime.

Authority to Act

LEAs will require appropriate authorisation to take actions (such as deploying tools) to conduct effective online investigations. Such authorisation needs to be framed to consider the dynamic and international nature of cyber crime. In particular, authorisation needs to be available in a timely fashion, given the perishable nature of most digital evidence. Authorisation should also consider that the trail leading to the attacker may pass through multiple national boundaries. In many instances, authorisation is likely to be required within 24 hours to be effective. This sort of timescale is the reality of digital investigations. Any system which does not provide such an enabling framework will simply not be effective.

The scale and complexity of jurisdictional issues means that national leadership and international cooperation are required. National governments need to provide the legal and policy framework to enable local LEAs to conduct effective digital investigations, acknowledging that these will almost always cross borders. This legislative framework needs to be flexible enough for the inevitable development of the digital landscape at a pace that far outstrips the tempo of the lawmaking process. Authority for operational approval should be handled at a level where deployment can happen swiftly and locally, based on broad parameters of necessity and proportionality, rather than specific tool sets or systems. The EC proposal on e-evidence refers to this as "direct access to e-evidence,"[13] an area which would need to be prioritised.

12 Imperva (2017). Beyond Takeover--Stories from a Hacked Account.

13 European Commission (June 11, 2017). How can we improve cross-border access to e-evidence?

International cooperation should acknowledge the realities of digital investigations, and the ineffectiveness of current mechanisms to deal with them. The timescale for a European Investigation Order, for instance, would be too great for many cyber crime cases where logs disappear in hours or days.[14] This should pave the way for an agreement that LEAs can conduct non-disruptive and proportionate intrusions during "active" pursuit of attackers, even when the systems involved may be based in a foreign jurisdiction. This could be accomplished, for instance, through an amendment to the Budapest Convention. A draft bill in the US Congress, known as the Active Cyber Defense Certainty Act,[15] sets out a framework for many of the relevant issues, including allowances for the deployment of "attributional technology" where it does not result in the destruction of data, impair the essential operating functionality of the target's computer system or intentionally create a backdoor enabling intrusive access.

The end state should be a system whereby LEAs are empowered, via swift and local authorisation, to pursue the trail left by attackers through third party systems in a similar way to entering private property without a warrant when in physical pursuit of a suspect or when they have reasonable grounds to believe that the person they are searching for is on the premises. Such an approach, within defined legislative parameters that provide for non-disruptive tracking activity only, is entirely necessary and absolutely proportionate in a world where up to half of all crime is committed online and will almost always cross borders. The approach is also self-selecting — although the profiler could potentially be intrusive, the operational methodology for its deployment ensures it will only be used against attackers. There may be some collateral intrusion (for example, where attackers are using previously hacked victim machines for their current crime), but the nature of the information collected will be targeted and the impact on innocent parties strictly limited.

Public-Private Cooperation

LEA cooperation with industry is now well established, with many success stories involving information sharing and strategic operations. One example is the arrest of the Carbanak cyber crime mastermind.[16] Such cooperation must now be extended into the tactical sphere to have any significant long-term impact on cyber crime.

Cyber security companies such as FireEye frequently identify situations where corporate entities are subject to ongoing attacks (a "crime in progress"). Many organizations, or their third party cyber security providers, have sophisticated monitoring for such malicious activity, to provide foundational intelligence on the attack and attacker. These organizations are also experienced enough to triage such attacks to identify threats that merit LEA attention.

The police should work in partnership with these organizations to exploit opportunities to investigate, locate and identify organised criminal groups. By being agile and ready to respond quickly and efficiently to such opportunities, and using tools with appropriate authorisation, LEAs could change the balance against attackers. Even a small number of prosecutions would start to have a significant deterrent effect as attackers realised that LEAs were starting to respond to more than a small percentage of crimes.

Moving forward, LEAs could combine the strategic and tactical. For instance, if a police force had identified a particular malware campaign or financially motivated cyber crime group as a high priority target, they could work with the private sector to identify opportunities to conduct tactical operations. Due to the high volume nature of most cyber crime, cyber incident response organizations would almost certainly encounter a live opportunity against any high profile campaign or group of interest to LEAs. Once briefed on LEA strategic priorities, the organizations could then flag such opportunities for tactical engagement to help track attackers.

A proactive approach requires active and extensive cooperation between law enforcement and the private sector, the development of trusted relationships, and an understanding of one another's priorities and methods of working. And if LEAs want greater visibility into cyber crime, and enhanced opportunities to act against attackers, a proactive approach is the only viable model.

14 European Commission (May 22, 2017). As of today the "European Investigation Order" will help authorities to fight crime and terrorism.
15 115th Congress (October 12, 2017). H.R. 4036, Active Cyber Defense Certainty Act.
16 Europol (March 26, 2018). Mastermind behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain.

Conclusion

Cyber crime is an endemic issue that is growing in scale and complexity, and attackers currently hold significant advantages:

- They do not concern themselves with jurisdictional issues.
- Their technical capabilities are much more agile and adaptive, since they can ignore intellectual property and subvert legitimate tools.
- They are not encumbered with the policy and process of government institutions or agencies.

The overall pace of change in the digital world magnifies these advantages and provides an environment in which criminals flourish as they exploit and experiment with tools and techniques at an unprecedented rate to reinvent old crimes or create new ones. LEAs must adapt to address this threat because existing frameworks and approaches are simply inadequate. Transformation needs to be driven at a governmental level.

The permissive environment in which cyber criminals currently operate needs to be addressed, and the risk judgement for individuals considering cyber crime needs to be drastically rebalanced. Only a tiny percentage of digital crimes are investigated, and even fewer lead to successful prosecutions so there is little (if any) deterrent for cybercriminals. However, increasingly visible and effective action from LEAs would lead to a downward pressure on overall cyber crime as they continue to erode attacker trust in the ability to conduct large scale, non-targeted campaigns.

Such LEA action needs to be routine, approached strategically (for example, defining targets of interest or thresholds) and deployed tactically. In practice:

All police officers should have at least basic training in cyber crime investigations.

Tools that track attackers should be provisioned to facilitate attribution and prosecution. These tools need to be quickly deployable at scale and maintained with low resource requirement (money and time), such as a profiler.

Organizations should work closely with the private sector to identify and respond to opportunities to pursue attackers involved in a cyber crime in progress. Longer-term, this could develop into a proactive approach in which specific campaigns or criminal groups are targeted through their interactions with the private sector.

Although traditional investigative principles hold true in the digital world, they must be applied to operations conducted at an unprecedented pace. This requires a major shift in thought and bold action to properly equip LEAs and address the current void.

Learn more about Mandiant consulting services at **www.FireEye.com/services.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FireEye®