# the (451) group

## Anti-botnet entrant Umbra Data knows the power of the Dark Side [Intelligence]

**Analyst: Josh Corman**

There's a new player on the scene to help in the fight against botnets. **Umbra Data** approached the 451 Group to debut its Botnet Intelligence feed dubbed 'Dark Side Intelligence.' While it is clear that botnets exceed the reach of most legacy security controls, the cost and complexity of IT security and the poor economy have prevented most budget-constrained organizations from doing much about it. Umbra Data hopes to deliver the value of its botnet intelligence feed through more consumable form factors – selling to service providers and enhancing existing enterprise security appliances.

### The 451 Take

Botnets are clearly an issue. Now well beyond a spam platform, adaptive persistent adversaries (state and criminal actors) leverage botnet covert command and control (C&C) channels to exfiltrate intellectual property and other value. That said, very few people have the budget or the staff to add a net-new appliance to their arsenal. While there is some spending on anti-botnet products like those from Damballa and FireEye, we believe a greater portion of the market wants to leverage these capabilities but cannot justify another appliance to do so. In many CISO discussions, we hear 'I love the research, but can I consume this content via one of my existing appliance investments?' We've been encouraging the existing players to pursue licensing their content for some time now. Umbra Data is showing it has both botnet and market/budget intelligence. We're eager to see which security appliances embrace and partner with it – as well as how other anti-botnet players respond.

### Context

San Jose-based Umbra Data was founded in October of 2008; it quietly tiptoed out of stealth this spring. The small firm is angel-funded, having borrowed $1.5m. The lean team has about 10 people, with the bulk being technical. At the helm as CEO is Paul Moriarty. Prior to starting Umbra Data, Moriarty was a director of internet content security for **Trend Micro**. Also from Trend Micro is Umbra Data CTO Marc Evans. Evans was a senior software architect. Both claim they helped bring to market the first two commercial anti-botnet solutions while at Trend Micro – the InterCloud Security Service and the Botnet Identification Service.

## Technology

Umbra Data sells a botnet command and control intelligence feed. To collect and maintain this feed, it leverages globally deployed sensors, open source intelligence feeds, and its own brand of 'secret sauce' analysis to triage and render actionable that which is collected. The product of its research flow is an XML file – updated hourly.

Its research 'net' is composed of physical and virtual servers deployed globally. These servers are primarily deployed within service providers. Its sensors do a number of things, including looking to be infected, and participate within these botnets. Research is more on the botnets than the zombies themselves, but includes both. Umbra Data also monitors domain registration to anticipate and track potential C&C candidates. It also leverages data from domain name system root servers and other sources that it feels are more reliable than potentially altered victim DNS configurations. Umbra Data will also analyze the malware itself. It also leverages open source intelligence feeds from the likes of Shadowserver, ZeuS Tracker, **Team Cymru**, plus six others and counting. Umbra Data claims it uses these feeds to trigger a closer look, as well as to validate its original findings and scoring.

All of its analysis feeds into the triage and analysis. The rule set hovers around 30 (plus or minus a handful of) steps to categorize its list of actionable attributes. Umbra Data described three major buckets – malicious systems (block), legitimate but compromised systems (alert) and suspect systems (monitor). The 'block' list is confirmed bad actors. Consumers of the XML feed can confidently block these. The 'alert' category is also confirmed bad actors, but where analysis has found the presence of legitimate activity, it gives consumers of the feed the ability to act in accordance with policy or in a more deliberate way – so as not to disrupt critical healthy activity. The last category flags suspect systems. This information, when combined with other actionable intelligence, may in fact lead to blocking. For example, a network data-loss-prevention appliance sees sensitive outbound information, but fears blocking legitimate business traffic. If the DLP appliance is enriched with the Umbra Data feed, policy decisions could allow the enterprise security team to opt to block the egress to bad, mixed or suspect actors, where broad blocking may not be practical.

## Products

Simply put, the Umbra Data product is its XML intelligence feed. The product was made available for sale in Q3 of 2009, and is named Dark Side Intelligence – not to imply Umbra Data is in league with the Emperor or Darth Vader. The feed is to enable better security decisions and policy enforcement with actionable intelligence about malicious 'Dark Side' command and control activity. The potential value of such a feed can be rendered kinetic by its consumers, with the stored energy being put into action. This is not unlike the cases described in our recent report on how **Qinetiq/Cyveillance** is being leveraged by existing network security platforms like intrusion-prevention systems – or in the Qinetiq example, like Fidelis XPS.

The Dark Side Intelligence XML feed is updated roughly hourly, but updates are soon to be more frequent. In addition to the feed, Umbra Data offers a Web portal to its clients. This

allows for interaction and queries of the XML content, as well as historical trending over time.

Pricing for Dark Side Intelligence ranges from $50,000-350,000. For service providers, pricing is based on the number of peering sites. For enterprises, the pricing is more based on the size of the organization. At the time of our briefing, Umbra had just inked a deal to deliver its content with a network security platform.

During its stealth period, Umbra Data went deep into honing the product with its first three paying clients – an Ivy League University, a service provider and its soon-to-be-announced OEM partner. Umbra Data found the university environment to be a microcosm of service-provider environments. Student-owned equipment paired with risky computing and poor hygiene (computer, of course) translates into fertile soil for zombie and botnet activity. It expects its service-provider clients to primarily leverage the clearly bad 'block' IPs from the Dark Side Intelligence feed. In enterprise environments where deep-packet-inspection appliances are able to leverage more granular blocking, it expects leverage of 'block' and 'alert' to inform traffic filtering based on policy.

Umbra Data has a number of active trials of Dark Side Intelligence, including several large and tier one ISPs. It is hopeful its freshly inked OEM deal will also bear fruit once it becomes public.

**Strategy**

The strategy is not to create yet another network security appliance. The optimal target mix of customers is to see 45-50% of uptake in the service-provider space. It hopes for 30% of its revenue to come from OEM relationships with other existing security partners. The remainder would be enterprises to consume directly – to feed into ESIM or other security operations.

The sensor footprint is global, and Umbra has two active trials outside of the US. Given the nature of its feed, sales will be via a mix of direct and third-party OEM/channel relationships.

**Competition**

Since Umbra Data is just now stepping out of stealth, competition is mostly conceptual at this point. Many of these existing approaches are complementary, but given tight budgets and the fact that it is not on the list of PCI's 'chosen few', it absolutely competes for scarce dollars. When you mention anti-botnet, primary competition is likely to come from **Damballa** and **FireEye**. Damballa does some excellent research, and is mainly consumed as an appliance. FireEye leverages virtualization to help identify new malware involved in botnets. Both are mostly focused on enterprise sales, although **Comcast** recently announced its use of Damballa. We expect service providers will consume more than one anti-botnet product or intelligence feed. We also expect that if Umbra Data is successful, Damballa should follow more aggressively.

For those looking for **Pramana** as a competitor, it appears to have closed shop on September 1. Although not there anymore, the website had said that Pramana's services would conclude at the end of September 1, 2010.

Other partial competition comes from the usual suspects in the anti-malware arena. **Symantec** and **McAfee** (now a division of **Intel**) claim they better handle botnets now with their suites of products and cloud research. Trend Micro brought early anti-botnet capabilities to market.

There are myriad competing and complementary open source and for-pay intelligence feeds, but those who consume one tend to consume many. Some of these include the aforementioned Qinetiq (Cyveillance), which offers various useful feeds for anti-phishing, anti-malware, site-safety index and identity-theft protection. **MarkMonitor** and **BrandProtect** have intelligence to protect your brand – with the former also doing some anti-phishing.

One interesting competitive twist comes from Umbra Data's strategy to only deliver a feed. Currently, if an enterprise has only enough budget for one or two more noncompliance-mandated projects, anti-botnet appliances compete for that slot with data-loss prevention, next-generation firewalls, network forensics and packet-capture appliances, as well as other one-function, 'uni-tasker' appliances. Umbra Data has already signed an OEM relationship with one such player. This could make any or all of those vendors potential partners. This changes the equation for those CISOs who wanted the anti-botnet capabilities, but didn't want a solo appliance for it. It could force the question, why buy an anti-botnet-only appliance if I can buy a box that does DLP and botnet C&C? The proof will be in the pudding.

Stand-alone DLP partners could include **Fidelis Security Systems**, **Code Green Networks**, **Blue Coat Systems**, **Websense**, **Trustwave** (**Vericept**) and **GTB Technologies** – not to mention (maybe) suite vendors like McAfee, Symantec, Trend Micro, **Sophos**, **IBM**, **Cisco**, **CA Technologies**, **RSA** and the like.

Network Forensics platforms like **NetWitness**, **Solera Networks**, **AccessData Group** (**SilentRunner**), **Niksun** and others can be used to spot suspicious traffic, and may be enriched by an Umbra Data feed. **MANDIANT's** Incident Response product could leverage the XML feed, in addition to its integration with application whitelist vendor **Bit9**, to help narrow the focus of incident-response exercises and add further context to potentially compromised system files. UTM, mail gateways and IPS players like **Fortinet**, **Barracuda Networks**, **SonicWALL**, **Astaro**, **Juniper Networks** and others could also benefit.

ESIM vendors, such as **NitroSecurity**, **TriGeo**, **AlienVault**, **LogRhythm**, **netForensics**, **LogLogic**, **S21Sec**, **Tier-3**, **Tenable Network Security**, **Alert Logic**, **Quest Software**, RSA (enVision), **Q1 Labs**, **Prism Microsystems**, **SenSage** and **eIQnetworks**, could benefit from the added intelligence feed to help add context to attacks and enrich existing correlation rules. Portfolio ESIM players, such as CA, IBM, **Novell**, Symantec, Trustwave and **Hewlett-Packard** (with its recent **ArcSight** acquisition) could also benefit. For that

matter, MSSPs would also make sense – including IBM, Symantec, **Verizon Business**, **AT&T**, **SecureWorks**, **Perimeter eSecurity**, **Solutionary**, Trustwave, **StillSecure**, **BT Counterpane**, **Wipro** and others.

Finally, while writing this report, the 451 Group was approached for a briefing by a pre-launch player for something looking quite a bit like Umbra Data. Look for that report in the near future.

**SWOT analysis**

| Strengths | Weaknesses |
|---|---|
| This lean team has prior anti-botnet chops. The licensed-content choice shows recognition of the spending climate, keeps it away from heavy capital dependencies and keeps focus squarely on the caliber of research. | Umbra Data is a small, early team with a niche offering in a check-box spending climate. |
| **Opportunities** | **Threats** |
| An 'Intel inside' or Autonomy model could get Dark Side Intelligence ubiquity in service providers and with many network security appliances in need of capabilities. We also believe ESIMs and MSSPs may find this an easy investment. | Good-enough perceived capabilities in existing security investments and free open source might drive down price or adoption. Licensing may prove easy to replicate for appliance competitors. |

For additional information on The 451 Group or to apply for trial access, go to: www.the451group.com