白皮書

具有IP智能的動態邊界安全

2014年8月8日更新

介紹

捍衛現代企業網絡邊界的完整性是一項艱鉅的任務。安全架構師必須應對諸如網絡釣魚引起的客戶資產損失，黑客入侵造成的數據洩露以及通過惡意軟件分發造成的高級持續威脅之類的威脅。

網絡釣魚

網絡釣魚已成為金融組織面臨的最大威脅之一。APWG互聯網政策委員會關於網絡釣魚的報告指出，在2010年有所減少之後，網絡釣魚攻擊在2011年再次上升。[1] 今天，金融組織對網絡釣魚所造成的財務損失和公眾認知損害尤為敏感，他們在努力工作尋找有效的解決方案。

數據洩露

隨著組織受到來自全球匿名代理的攻擊者的滲透，數據洩露仍然是備受關注的新聞報導。Verizon和美國特勤局的研究人員大開眼界的報告顯示，2010年，50%的數據洩露利用某種形式的黑客攻擊，而49%的惡意軟件利用了某種形式的惡意軟件。[2]

高級持續威脅

現代惡意軟件可以感染附近的主機，攻擊外部目標，生成垃圾郵件並參與高級持久威脅（APT）活動。

威脅向量	**結果**
惡意軟件	違反，數據丟失
網絡釣魚	客戶資產損失
掃描儀	網絡偵察
殭屍網絡	高級持續威脅

圖1： 當今的威脅可能會導致許多問題，從而導致災難性的損失。

面對這些威脅，保護網絡邊界是一項艱鉅的任務。部署防火牆，掃描漏洞，緩解網絡DDoS攻擊並集成Web應用程序防火牆（WAF）之後，仍然存在一個重大問題：無論企業網絡多麼安全，外部Internet上的主機可能都不安全。但是哪個主機？如何授權出站連接？如何智能地評估入站請求？

們必須考慮每個出站Internet目標地址的聲譽。其中一些地址映射到惡意主機，例如網絡釣魚代理或殭屍網絡服務器。傳入連接可以來自活動，惡意或可疑地址，例如匿名出口節點或掃描儀。

為了幫助IT組織解決此項目，F5提供了一組新的面向上下文的服務，包括IP智能，這對於製定有關流量管理的動態決策至關重要。

歡迎使用IP Intelligence

F5產品組合長期以來為網絡提供情報和敏捷性而聞名。BIG-IP系統的新功能是BIG-IP全球交付智能，它可以根據上下文增強交付決策。具有IP Intelligence的BIG-IP全球交付智能服務可保護企業範圍免受惡意Internet主機的攻擊。BIG-IP全球交付智能還向諸如BIG-IP全球流量管理器（GTM）提供的服務提供基於位置的數據。

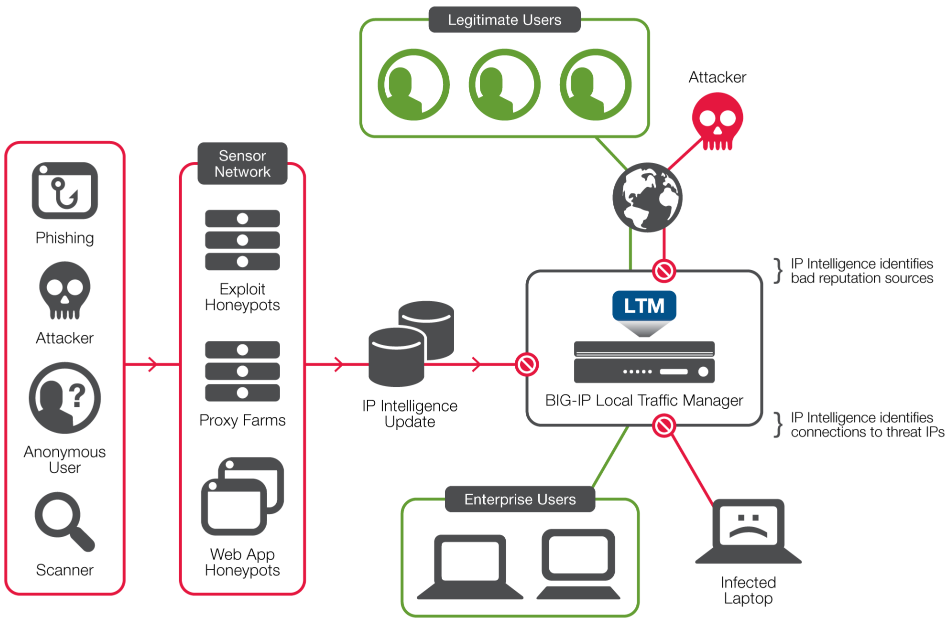


圖2：IP Intelligence收集信譽數據以供F5解決方案使用。

IP Intelligence內置在位於網絡外圍的F5 ADC中，可保留有關Internet上超過一百萬個惡意地址的信息，並可阻止與這些地址之間的連接。該地址數據庫每隔五分鐘從雲中刷新一次，以最大程度地減少威脅窗口並保持組織數據及其聲譽的安全。

IP智能技術的背後是一個全球威脅傳感器網絡，其組成為：

- 半開放式代理服務器場
- 利用蜜罐
- 天真的用戶模擬
- Web應用程序蜜罐
- 第三方資源

這些傳感器組件捕獲事件數據並將其提供給威脅分析網絡，該網絡會生成IP Intelligence主機數據庫，並為每個條目分類。

網絡釣魚

accounts are still a primary phishing target, but the latest trend is for attackers to capture credentials that lead not only to e-commerce sites, but to any site where there is potential financial gain. For example, registered accounts with which users enter credit card numbers to purchase retail items are especially attractive targets. So far, banks have been covering these losses instead of passing them on the consumer; but the costs of phishing are growing every year, and organizations must seek better ways to mitigate this ongoing threat.

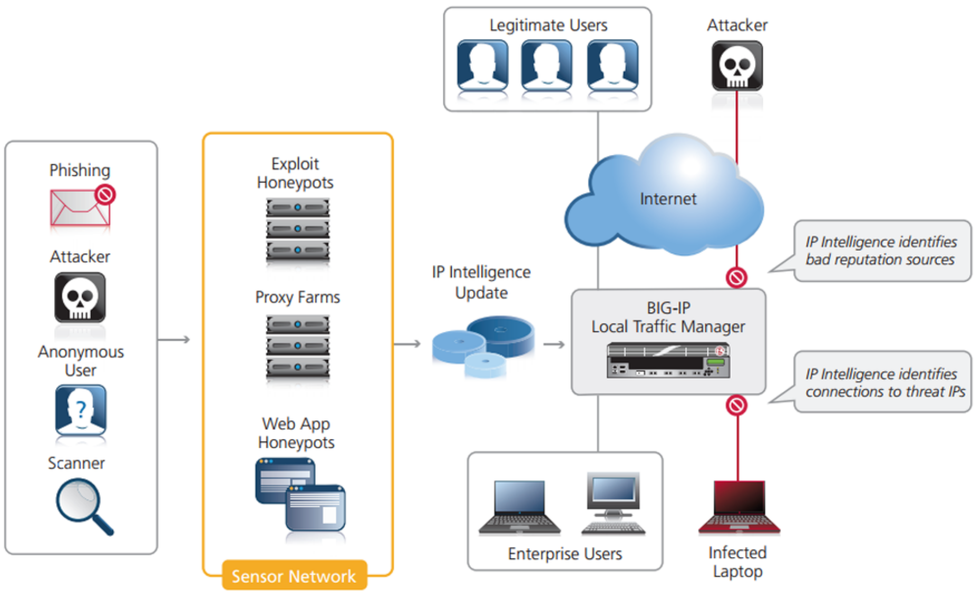


Figure 3: IP Intelligence separates legitimate users from phishing proxies.

Phishing is to some degree a social engineering technique, in that it fools the victim into thinking they are connecting to their bank. Because most sites with financial assets use SSL certificates to secure the connection, the phishing attacker must trick the victim into connecting to a phishing proxy site for which they have a certificate that looks like the user's target site, but whose URL doesn't really match. This prevents the browser from displaying an alert. As long as the victim is not paying close attention to the browser bar, the attack will succeed at the phishing proxy.

IP Intelligence tracks known phishing proxies, allowing BIG-IP users to prohibit malicious requests from phishing sites, such as man-in-the-middle attacks, or to respond with an alert.

Anonymous Proxies

Anonymous proxy networks, like The Onion Routing (TOR) project, mask network traffic source information using network graphs and multiple levels of encryption. Traffic that passes through the anonymous network will arrive at its destination, but without the original source address. The payload has also been mixed with other traffic and bounced around enough nodes to add delay and repudiation on the behalf of the sender. Traffic coming from these exit nodes may have originated anywhere and is, of course, very difficult to trace.

senders are oppressed citizenry evading dictatorial review; but more often they are hackers or other malicious agents.

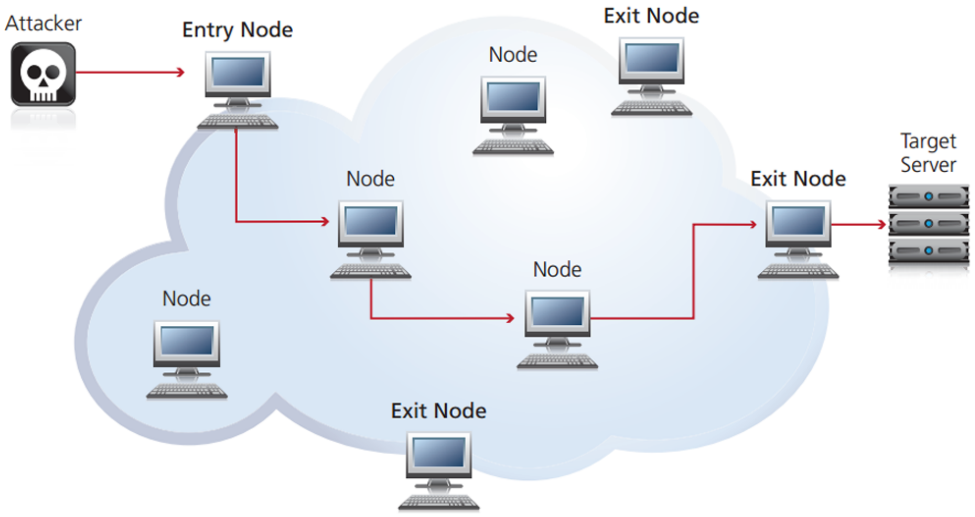


Figure 4: An attacker can mask his or her source by using anonymous proxy network.

While some legitimate use cases do exist, one fact cannot be denied: the best malicious hackers in the world use anonymous networks to hide their locations. In June 2011, one of the world's most wanted hackers was finally apprehended when he neglected to mask his source address a single time.

It's critical for enterprises to prevent these individuals from connecting to their networks by implementing a policy prohibiting, or at least discouraging, connections from known anonymous networks. Because IP Intelligence knows, in near real time, which Internet addresses represent the exit nodes of the anonymous network relays, it can successfully block connections from them.

Scanners

Scanners are more dangerous than they appear at first glance. Scanners attempt to connect to different hosts and ports at the enterprise. They often connect but fail to authenticate, or they speak the wrong protocol and appear to give up and go away. The real result though, is that they are gathering reconnaissance data for use in later attacks.

Scanners perform reconnaissance for:

- Conventional network attacks
- Low-bandwidth asymmetric application attacks
- Web application security vulnerabilities

Scanners and Application Attacks

Scanners have always been used to lay the foundation for a conventional network attack, but they've evolved to perform reconnaissance for two forms of application attacks. The first is a new class of low-bandwidth asymmetric attacks. Attackers use scanners to recursively query a website and measure the time interval that certain expensive queries that the site offers, leading to a denial of service at the database level. This attack is extremely difficult to detect because it does not involve a heavy spike in incoming traffic.

The second type of reconnaissance has seen a massive uptick in the last two years. Attackers have been probing web applications for vulnerabilities such as SQL injections and cross-site scripting. They can then catalogue and sell the data they retrieve, or else use it in a subsequent application attack.

In the BIG-IP system, IP Intelligence stops this class of attacks by preemptively preventing known scanning hosts from connecting to the site. If scanners attempt to evade detection by using anonymous proxies, they will still be denied because IP Intelligence knows about those networks as well. If the scanner attempts to evade detection by setting up a new scanning host, that host address will become known through the IP Intelligence threat analysis network, and will subsequently appear in the IP Intelligence database within five minutes.

Botnet Command and Control

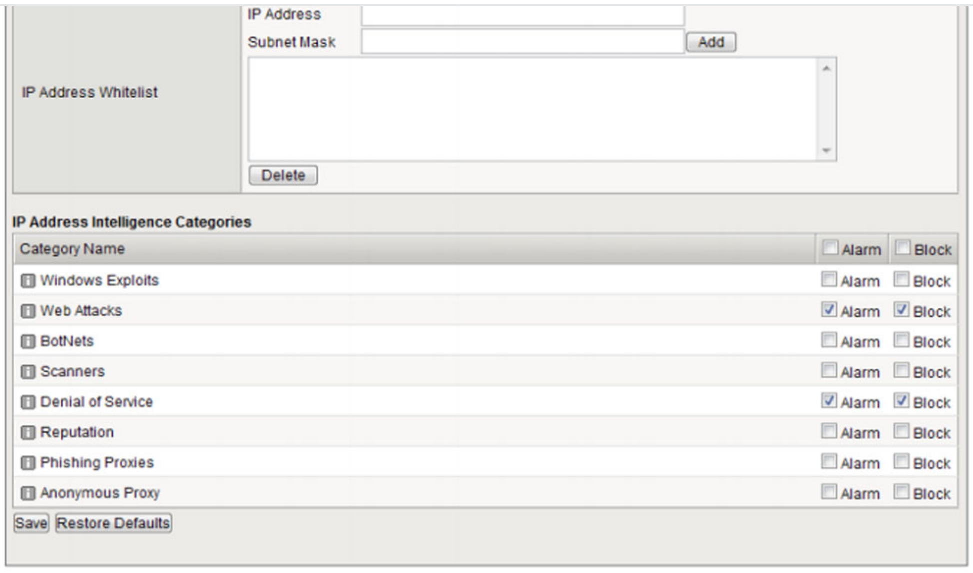
Today's malware can generate enormous amounts of spam, infect nearby hosts, attack external targets via DDoS, and participate in advanced persistent threat (APT) activities. If a device inside the enterprise perimeter is infected with malware and becomes part of a botnet, it may show itself by attempting to connect to a command-and-control (C&C) host on the Internet in order to receive attack orders. The threat analysis network behind IP Intelligence tracks known botnet C&C hosts and includes them in its reputation database.

An administrator can designate virtual servers for outgoing traffic to watch for specific destination ports and then trap and log connections to known botnet C&C hosts. The log indicates which internal devices are infected so administrators can initiate remediation measures.

There are new botnets every day, and their C&C hosts are constantly changing. This necessitates the use of an intelligent threat analysis network like the one behind IP Intelligence. The automatic updates that occur every five minutes to the IP Intelligence database within the BIG-IP system minimize the threat window.

IP Intelligence Control

With BIG-IP Application Security Manager (ASM), IP Intelligence will block incoming connections whose source addresses match its database. A whitelist can be configured by the administrator to bypass IP Intelligence for the selected address in the list.



IP Address Whitelist

IP Address

Subnet Mask

IP Address Intelligence Categories

Category Name	□ Alarm	□ Block
Windows Exploits	□ Alarm	□ Block
Web Attacks	☑ Alarm	☑ Block
BotNets	□ Alarm	□ Block
Scanners	□ Alarm	□ Block
Denial of Service	☑ Alarm	☑ Block
Reputation	□ Alarm	□ Block
Phishing Proxies	□ Alarm	□ Block
Anonymous Proxy	□ Alarm	□ Block

Figure 5: IP Intelligence includes a whitelist for fine-grain control.

BIG-IP ASM presents IP Intelligence usage in an easy-to-use GUI. IP Intelligence is also available for use with F5's iRules scripting language, which allows IT organizations to customize their evaluation to their needs.

```
    # Setup High-Speed Logging

    set hsl [HSL::open -proto UDP -pool
syslog_server_pool]

}

when HTTP_REQUEST {


    set ip_reputation_categories [IP::reputation
[IP::client_addr]]

    set is_reject 0



    if {($ip_reputation_categories contains “Windows
Exploits”)} {

        set is_reject 1

}


if {($ip_reputation_categories contains “Web
Attacks”)} {

    set is_reject 1

}


if {($is_reject)} {

   HSL::send $hsl “Attempt access from malicious ip
address [IP::client_addr]
($ip_reputation_categories), request was rejected”

    HTTP::respond 200 content “

The request was rejected.
Attempt access from malicious ip address

” } }
```

Networks

IP Intelligence can provide its defensive services even when used with a content delivery network (CDN). IP Intelligence can evaluate the original IP address in the X-Forwarded-For (XFF) header. Other solutions, such as intrusion prevention systems (IPSs) or conventional firewalls, examine the source address of the packets and mistakenly evaluate the reputation of the CDN's proxy address rather than correctly evaluating the reputation of the original client source address.

Conclusion

Attack methodologies change. Threat vectors change. Once-powerful defenses become obsolete. As the pace of these changes increases, it's unrealistic to wait for defense methods to catch up, or for new products to be developed and releases pushed out. Financial enterprises need near real-time host protection, where the bad actors are known to the rest of the world even as they act.

The BIG-IP system and the IP Intelligence service at the security perimeter provide the up-to-date network threat intelligence that is independent of attack type. If a new criminal actor attacks this today, the IP Intelligence database will begin providing protection from the hosts involved within minutes.

IP Intelligence provides protection against phishing, defends against anonymous attackers and scanners, and blocks botnet control. By leveraging IP Intelligence in their BIG-IP deployments, financial organizations can minimize the threat window and protect valuable enterprise assets.

[1] Global Phishing Survey: Trends and Domain Name Use in 2H2010. APWG Internet Policy Committee, April 2011.

[2] 2011 Data Breach Investigations Report. Verizon RISK Team, 2011.

48 of the Fortune 50 rely on F5

85 offices in 43 countries

20 plus years protecting apps

ABOUT F5

Corporate Information
Newsroom
Investor Relations
Careers
Contact Information
Communication Preferences
Product Certifications
Diversity & Inclusion

EDUCATION

Training
Professional Certification
LearnF5
Free Online Training

F5 SITES

F5.com
DevCentral
Support Portal
Partner Central
F5 Labs

Trademarks Policies Privacy California Privacy 不要出售我的個人信息 Cookie喜好設置