AGILITY
2016
SOLUTIONS FOR AN APPLICATION WORLD
How F5 Helps Customers Facing DDoS Attacks and Threats

Ted Nixon
Manager, Global Services Sales

Stephen Kiel
Security Specialist
A New Perimeter Requires New Defenses

Applications are exposed from end to end
A New Perimeter Requires New Defenses

Applications are exposed from end to end

The Problem:
A New Perimeter Requires New Defenses

Applications are exposed from end to end

The Problem:
Distributed Denial of Service (DDoS) attacks are bad and getting worse.
A New Perimeter Requires New Defenses

Applications are exposed from end to end

The Problem:
Distributed Denial of Service (DDoS) attacks are bad and getting worse.

The Challenges:
A New Perimeter Requires New Defenses

Applications are exposed from end to end

The Problem:
Distributed Denial of Service (DDoS) attacks are bad and getting worse.

The Challenges:
How can you leverage and strengthen your relationship with the customer while solving an immediate threat that could cause critical downtime?
A New Perimeter Requires New Defenses

Applications are exposed from end to end

The Problem:
Distributed Denial of Service (DDoS) attacks are bad and getting worse.

The Challenges:
How can you leverage and strengthen your relationship with the customer while solving an immediate threat that could cause critical downtime?
A New Perimeter Requires New Defenses

Applications are exposed from end to end

The Problem:
Distributed Denial of Service (DDoS) attacks are bad and getting worse.

The Challenges:
How can you leverage and strengthen your relationship with the customer while solving an immediate threat that could cause critical downtime?

The Solution:
A New Perimeter Requires New Defenses

Applications are exposed from end to end

The Problem:
Distributed Denial of Service (DDoS) attacks are bad and getting worse.

The Challenges:
How can you leverage and strengthen your relationship with the customer while solving an immediate threat that could cause critical downtime?

The Solution:
DDoS Attacks:
From Bad to Worse
DDoS Attacks Motivators

Accidents  Fame  Extortion  Vandalism
Business Competition  Nihilism  Misconfiguration
Politics  Publicity  Ideology  Experiments
Financial Market Manipulation  Retaliation/Revenge
Entertainment  Hacktivism  Notoriety
Inter-Personal/-Group Rivalry  Distraction/Diversion

In other words:

Money, Protest, Mischief, Rivalry, Incompetence, or Narcissism
In other words: Money,
DDoS Attacks Motivators

- Accidents
- Fame
- Extortion
- Vandalism
- Business Competition
- Nihilism
- Misconfiguration
- Politics
- Publicity
- Ideology
- Experiments
- Financial Market Manipulation
- Retaliation/Revenge
- Entertainment
- Hacktivism
- Notoriety
- Inter-Personal/-Group Rivalry
- Distraction/Diversion

In other words: Money, Protest,
DDoS Attacks Motivators

- Money
- Protest
- Mischief
- Rivalry
- Incompetence
- Narcissism
- Retaliation/Revenge
- Inter-Personal/-Group Rivalry
- Financial Market Manipulation
- Business Competition
- Politics
- Publicity
- Extortion
- Nihilism
- Misconfiguration
- Experiments
- Ideology
- Entertainment
- Hacktivism
- Notoriety
- Distraction/Diversion

In other words: Money, Protest, Mischief,
In other words: Money, Protest, Mischief, Rivalry,
## DDoS Attacks Motivators

<table>
<thead>
<tr>
<th>Accidents</th>
<th>Fame</th>
<th>Extortion</th>
<th>Vandalism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Competition</td>
<td>Nihilism</td>
<td>Misconfiguration</td>
<td></td>
</tr>
<tr>
<td>Politics</td>
<td>Publicity</td>
<td>Ideology</td>
<td>Experiments</td>
</tr>
<tr>
<td>Financial Market Manipulation</td>
<td></td>
<td></td>
<td>Retaliation/Revenge</td>
</tr>
<tr>
<td>Entertainment</td>
<td>Hacktivism</td>
<td></td>
<td>Notoriety</td>
</tr>
<tr>
<td>Inter-Personal/-Group Rivalry</td>
<td></td>
<td></td>
<td>Distraction/Diversion</td>
</tr>
</tbody>
</table>

In other words: Money, Protest, Mischief, Rivalry, Incompetence,
## DDoS Attacks Motivators

<table>
<thead>
<tr>
<th>Accidents</th>
<th>Fame</th>
<th>Extortion</th>
<th>Vandalism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Competition</td>
<td>Nihilism</td>
<td>Misconfiguration</td>
<td></td>
</tr>
<tr>
<td>Politics</td>
<td>Publicity</td>
<td>Ideology</td>
<td>Experiments</td>
</tr>
<tr>
<td>Financial Market Manipulation</td>
<td></td>
<td></td>
<td>Retaliation/Revenge</td>
</tr>
<tr>
<td>Entertainment</td>
<td>Hacktivism</td>
<td></td>
<td>Notoriety</td>
</tr>
<tr>
<td>Inter-Personal/-Group Rivalry</td>
<td></td>
<td></td>
<td>Distraction/Diversion</td>
</tr>
</tbody>
</table>

In other words: **Money, Protest, Mischief, Rivalry, Incompetence, or Narcissism**
In other words: Money, Protest, Mischief, Rivalry, Incompetence, or Narcissism
Threats Today: Hacktivism

Using and abusing technology to affect social change
Threats Today: Hacktivism

Using and abusing technology to affect social change
Threats Today: Hacktivism

Using and abusing technology to affect social change

Hacktivism is a form of cyber terrorism

• Rooted in hacker culture—i.e., hacker activism.
• Usually related to free speech, human rights, or freedom of information.
Threats Today: Hacktivism

Using and abusing technology to affect social change

Hacktivism is a form of cyber terrorism
• Rooted in hacker culture—i.e., hacker activism.
• Usually related to free speech, human rights, or freedom of information.

Anonymous is synonymous with hacktivism
• “Anonymous has a very loose and decentralized command structure that operates on ideas rather than directives.”*
• Their activities have evolved over time from making prank phone calls, to sending black faxes, to launching DDoS attacks.

Threats Today: Hacktivism

Recent Anonymous DDoS targets

March 2016
ISIS, Donald Trump (again), NASA, Oakland County Republicans

April 2016
Angolan, Ku Klux Klan, Black Lives Matter, Israel, Denmark, Iceland, Dalhousie University, Italy

May 2016
Multiple global financial institutions, North Carolina

June/July 2016?
The DDoS extortion model is proven:

1. Threaten a company with a major Distributed Denial of Service attack.
2. Execute an immediate warning DDoS attack as proof of intent and capability.
3. Demand a payment (usually in Bitcoin) to prevent a future massive DDoS attack.
4. Follow up with further threats to heighten the fear.
Threats Today: DDoS Extortion

Pay up or be taken down

The DDoS extortion model is proven:

1. Threaten a company with a major Distributed Denial of Service attack.
2. Execute an immediate warning DDoS attack as proof of intent and capability.
3. Demand a payment (usually in Bitcoin) to prevent a future massive DDoS attack.
4. Follow up with further threats to heighten the fear.

Why use Bitcoin?

It is a new and unregulated currency that allows extortionists to accept payments anonymously.
Threats Today: DDoS Extortion
New DDoS extortionists emerge using the same old tricks (and names)

DD4BC (DDoS for Bitcoin)—Mid 2014
Attacked 140+ companies; Suspects arrested by Europol in January 2016.

Armada Collective—Fall 2015/Spring 2016
Attacked dozens of companies and growing.

Caremini—Spring 2016
Multiple German companies threatened to pay “charity donations.”

More greedy copycats and impersonators continue to appear
Some threats are not even reinforced with warning attacks!
Threats Tomorrow: ?

Today’s young online gamers may become tomorrow’s DDoS extortionists
Threats Tomorrow: ?

Today’s young online gamers may become tomorrow’s DDoS extortionists
Threats Tomorrow: ?

Today’s young online gamers may become tomorrow’s DDoS extortionists
Threats Tomorrow: ?

Today’s young online gamers may become tomorrow’s DDoS extortionists

Online Stresser/Booter service
Threats Tomorrow: ?

Today’s young online gamers may become tomorrow’s DDoS extortionists

Online Stresser/Booter service

Cyber attack how-to guides released by Anonymous to target ISIS websites in November 2016 in response to the Paris bombings
Threats Tomorrow: ?

Today’s young online gamers may become tomorrow’s DDoS extortionists

Online Stresser/Booster service

Cyber attack how-to guides released by Anonymous to target ISIS websites in November 2016 in response to the Paris bombings
F5 Silverline
DDoS Protection Service
F5 Silverline DDoS Protection Service

Multiple deployment options

**Standalone Deployment**
No On-Premises Equipment Required
F5 Silverline DDoS Protection Service

Multiple deployment options

Standalone Deployment
No On-Premises Equipment Required

Hybrid Deployment
Leverage On-Premises BIG-IP Technology
F5 Silverline DDoS Protection Service

Multiple deployment options

**Standalone Deployment**
No On-Premises Equipment Required

**Hybrid Deployment**
Leverage On-Premises BIG-IP Technology
F5 Silverline DDoS Protection Service

Multiple service options
F5 Silverline DDoS Protection Service

Multiple service options
F5 Silverline DDoS Protection Service

Multiple service options

Always On
Primary protection as the first line of defense
- Stops bad traffic from ever reaching your network
- Continuously processes all traffic through the cloud-scrubbing service
- Delivers only legitimate traffic to your site

Always Available
Primary protection available on-demand
- Runs on stand-by
- Initiated when under DDoS attack
- Mitigates attack traffic on arrival
Cost Components of Service

Type of Service
• Always On
• Always Available

Clean Bandwidth
• Returned traffic during attack—95th percentile

Length of Term
• 1-year agreement
• 3-year agreement

Number of Assets Protecting
• # of DCs, VIPs

❑ The F5 Silverline Account Management team will assist you in scoping out the deal
F5 DDoS Hybrid Defender
Introducing F5’s New Standalone Security Product

F5 DDoS Hybrid Defender

- Integrated Layer 3 – Layer 7 DDoS Protection in one appliance
- Native behavioral analysis capabilities for sophisticated DDoS threat discovery
- Built-in SSL attack defense with support for termination and inspection of SSL traffic
- Bot detection for automated layer 7 DDoS defense
- Streamlined cloud off load of volumetric attack traffic
- Multiple BIG-IP platform choices and flexible hybrid deployment options
Example Hybrid On Premises/Cloud Deployment
F5 DDoS Hybrid Defender + F5 Silverline DDoS Protection Service

- Layer 3/Layer 4 DDoS mitigation in front of Firewall for small-medium volumetric DDoS attack protection
- Layer 7 DDoS mitigation with SSL termination behind Firewall for SSL and Protocol based DDoS attack protection
- Always Available (on-demand) Silverline Service with signaling for large-huge volumetric DDoS attack protection
F5 Emergency Onboarding Process
Emergency Activation of F5 Silverline Services

Working with a customer who is under DDoS attack (or being threatened)

If your customer calls you, do the following:

1. Contact F5
   - 24x7 live under attack hotline: 866-329-4253
   - Silverline sales team: AMERSilverlineSalesTeam@F5.com

2. Silverline specialist will engage with you and your customer

3. Deliver a quote and confirm the purchase
Engaging with the Dedicated Specialist Team

Breaking down the customer engagement with the Silverline Specialist Team

F5 Specialist Has Call with Partner and Customer

F5 Specialist Sends Service Terms to Customer

Customer Executes Service Terms

F5 SOC Completes Onboarding Process

F5 SOC Begins DDoS Attack Mitigation

Requirement Discovery
Scoping
Technical Q&A
Pricing
Next Steps Action Items
Engaging with the Dedicated Specialist Team

Breaking down the customer engagement with the Silverline Specialist Team

Service terms sent to customer through DocuSign (minimum 1-year commitment)
Engaging with the Dedicated Specialist Team

Breaking down the customer engagement with the Silverline Specialist Team

Customer signs terms via DocuSign
Partner confirms purchase of services by customer
Specialist authorizes provisioning to SOC
SOC sends provisioning email
SOC reaches out to customer for on boarding call (if necessary)
Provisioning begins
(15 minutes—proxy/4+ hours—routed)
Engaging with the Dedicated Specialist Team

Breaking down the customer engagement with the Silverline Specialist Team

- F5 Specialist Has Call with Partner and Customer
- F5 Specialist Sends Service Terms to Customer
- Customer Executes Service Terms
- F5 SOC Completes Onboarding Process
- F5 SOC Begins DDoS Attack Mitigation

Once provisioning complete and tested, traffic is redirected to Silverline
HipChat or conference call is opened
Scrubbing begins
A retail customer of CompuNet, a 2015 Unity Rising Star Partner of the Year, received a low level and threatening ransom demand email from the Armada Collective.

- Rather than pay the demand which expired in 24 hours, this customer relied on their trusted reseller to offer a solution which will allow them to meet their **stringent technical requirements**, engage in their purchase process, and complete provisioning before the attack deadline.

“First Call at Noon… PO signed by 6:00 routing traffic by 8:00, all traffic converged and routing through Silverline by 9:30. If that isn’t a story we can sell, I don’t know what is. The F5/Silverline experience was unbelievable. I frankly cannot believe that this kind of an experience was possible.”

-Robert Elsethagen, Consulting Engineer, CompuNet, Inc.
Action Items

Start your preparations now and be ready to go

Plant Seeds

Educate customer base on their options
Position yourselves and F5 as the first point of contact
Discuss the benefits of being proactive

Continue to Water

Continually drip feed your customers DDoS information so that they think of you and F5 in their time of need
Give Feedback – Get Points!

• Add class to your personal schedule.
• Survey will pop up in Mobile App.
• Answer the multiple choice.
• Submit your question to complete.
• Receive 5 points!