

2017'de Siber Güvenlik, Milli Çözümler ve Türkiye «NE'LER, NASIL'LAR»



Mustafa AFYONLUOĞLU

Siber Güvenlik, e-Yönetişim ve e-Devlet Kıdemli Uzmanı



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ




BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER


8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

2017'DE SİBER DÜNYA



VERİ SIZINTILARI	2014	2015	2016
Sızıntı Sayısı	1,523	1,211	1,209
Sızıntı başına Ortalama Veri Kaybı	805	466	927
Toplam Sızan Veri Adedi	1,200,000,000	564,000,000	1,100,000,000
10 Milyondan fazla kişiyi etkileyen olay sayısı	11	13	15

Son **8 Yılda** Sızan Veri Miktarı **7.1 MİLYAR KİMLİK**



FİDYE YAZILIMLAR	2014	2015	2016
Tespit Edilen Fidye Olay Sayısı	0	340,665	463,841
Fidye Yazılım Türü	30	30	101
Ödenen Ortalama Fidye (ABD Doları)	373	294	1,077



ORTALAMA	2016
Tarım, Ormanlık ve Balıkçılık	Her 1815 postada 1 tane
Finans, Sigortacılık, Kiralama	Her 1918 postada 1 tane
Madencilik	Her 2254 postada 1 tane
Kamu Yönetimi	Her 2329 postada 1 tane
En az: Taşımacılık ve Elektrik/Su gibi hizmetler	Her 6176 postada 1 tane

27 Nisan 2017 Symantec Corp. Internet Security Thread Report, Vol: 22



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

2017'DE SİBER DÜNYA

Saldırı Grubu	Kısa Adı	Ülke	Kuruluş Yılı	Motivasyonu	Hedef Kategoriler
Sandworm	Quedagh, BE2 APT	Rusya	2014	Casusluk, Sabotaj	Hükümetler, Uluslararası Organizasyonlar, Avrupa, Amerika, Enerji Sektörü
Fritillary	Cozy Bear, APT29, Office Monkeys	Rusya	2010	Casusluk, Hükümet Devirme, Yıkma	Hükümetler, Düşünce Örgütleri, Medya, Avrupa, Amerika
Swallowtail	Fancy Bear, APT28, Sednit	Rusya	2007	Casusluk, Hükümet Devirme, Yıkma	Hükümetler, Avrupa, Amerika
Cadelle	-	İran	2012	Casusluk	Havayolları, İletişim, İran Vatandaşları, Hükümetler, STK'lar
Appleworm	Lazarus	Kuzey Kore	2012	Casusluk, Sabotaj, Hükümet Devirme, Yıkma	Finans Sektörü, Askeriye, Hükümetler, Eğlence sektörü, Elektronik Cihazlar
Housefly	Equation	ABD	2001	Casusluk	Ülke saldırganlarına yönelik hedefler
Strider	Remsec	Batı	2011	Casusluk	Büyükelçilikler, Havayolları, Rusya, Çin, İsveç, Belçika
Suckfly	-	Çin	2014	Casusluk	e-Ticaret, Hükümetler, Teknoloji, Sağlık Sektörü, Finans Sektörü, Gemicilik Sektörü
Buckeye	APT3, UPS, Gothic Panda	Çin	2009	Casusluk	Askeri Alanlar, Savunma Endüstrisi, Medya, Eğitim Sektörü, ABD, İngiltere, Hong Kong
Tick	-	Çin	2006	Casusluk	Teknoloji, Yayıncılık, Japonya, Su Mühendisliği

Dikkat Çekici Etkileri Olan ve **Ülkeler Tarafından Desteklendiği Açıkça Bilinen** Hedef Odaklı Saldırı Grupları

27 Nisan 2017 Symantec Corp. Internet Security Threat Report, Vol: 22



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

SİBER GÜVENLİK ve MİLLİ GÜVENLİK

Milli Güvenlik: Devletin milli varlığına, bekasına ve güvenliğine yönelik tehditlere karşı tedbirler almak için **bölgesel** ve **küresel** ortamın izlenerek **tehdit** ve **fırsat**ların tespit edilmesi ile bu hususlara uygun siyasetin belirlenmesini ve en uygun politikaların uygulanmasını sağlayacak **süreç ve unsurlar** (MGK)*



2016 NATO VARŞOVA ZİRVESİ

2016: NATO Sistemlerine Saldırılar
Ayda **500** (2015'e göre %60 artış)

Ulusal Siber Güvenlik Bütçeleri
Fransa (2014): **1 Milyar €** UK: **2.5 Milyar €** (2016)

2030 Siber Güvenlik Hacmi: **90 Trilyon \$**
(Denver Üniversitesi)

* <http://www.mgk.gov.tr/index.php/milli-guvenlik-kurulu/genel-bilgi>

** <http://www.nato.int/docu/review/2017/Also-in-2017/Also-in-2017-nato-priority-spending-success-cyber-defence/EN/index.htm>



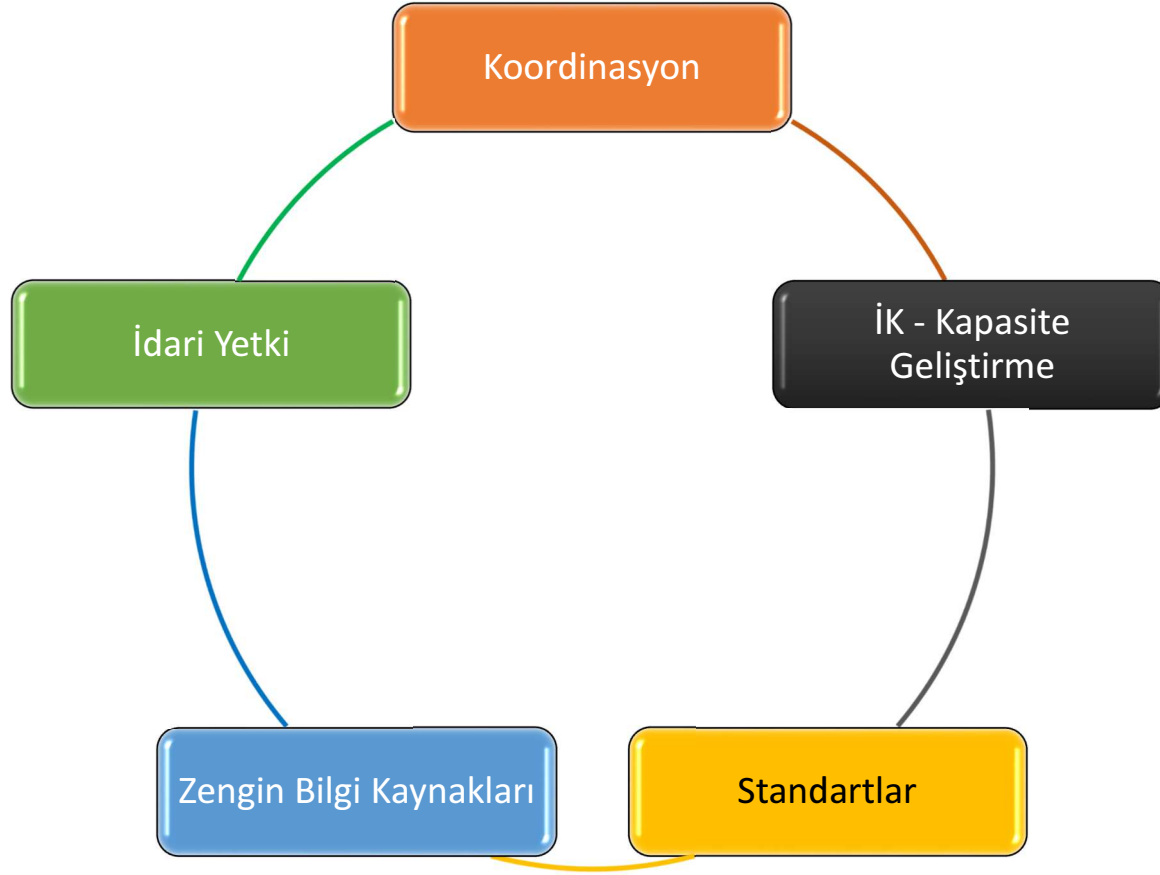
BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

SOME'ler ve Kritik Bileşenler: «Ne» Gerekliyor ?



«NASIL» ?

SİBER OLAYLARA MÜDAHALE EKİPLERİNİN KURULUŞ, GÖREV VE ÇALIŞMALARINA DAİR USUL VE ESASLAR HAKKINDA TEBLİĞ

11 KASIM 2013

Kurumsal SOME'lerin görev ve sorumlulukları

Madde 5: (2) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda **teknik ve idari tedbirler konusunda öneri sunarlar.**



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

SOME Nerede Konumlanmalı: Kurum İçi Yönetişim

MEVCUT DURUM



SOME Nerede Konumlanmalı: Kurum İçi Yönetişim

ÖNERİLEN İDARİ MODEL



«NASIL» ?

SİBER OLAYLARA MÜDAHALE EKİPLERİNİN KURULUŞ, GÖREV VE ÇALIŞMALARINA DAİR USUL VE ESASLAR HAKKINDA TEBLİĞ

11 KASIM 2013

Kurumsal SOME'lerin görev ve sorumlulukları

Madde 5: (2) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda **teknik ve idari tedbirler konusunda öneri sunarlar.**

(4) Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı **kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar.**



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



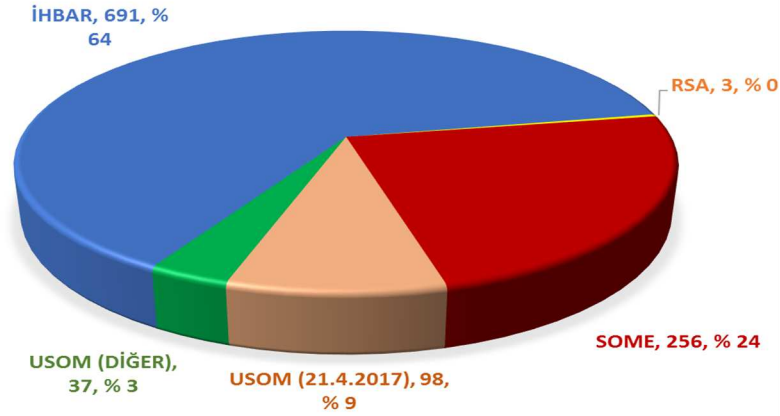
BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

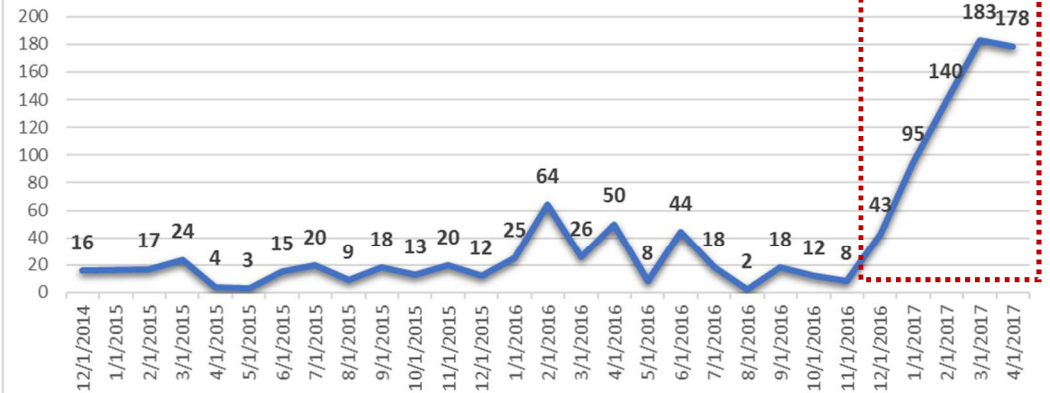
8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

SAYILARLA USOM

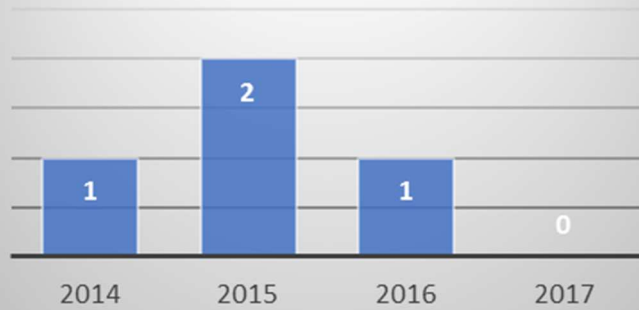
USOM TARAFINDAN YAYINLANAN ZARARLI BAĞLANTI LİSTESİ



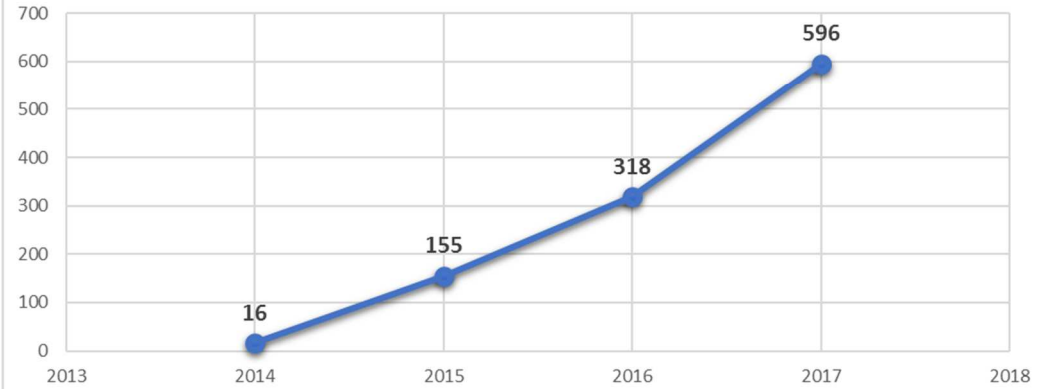
AYLAR BAZINDA YAYINLANAN ZARARLI BAĞLANTI ADEDİ



DUYURU ADEDİ



YILLAR BAZINDA YAYINLANAN ZARARLI BAĞLANTI ADEDİ



<https://www.usom.gov.tr/url-list.xml>



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



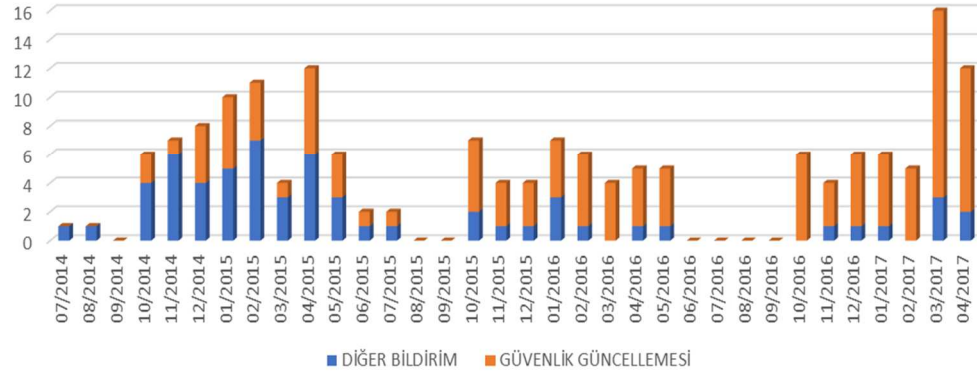
BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

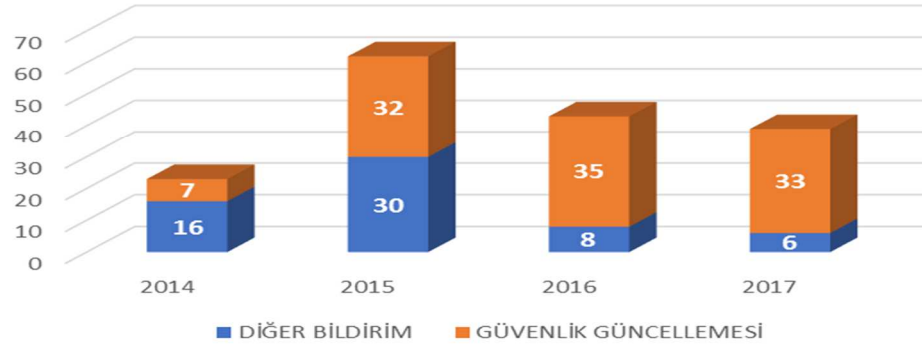
8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

SAYILARLA USOM

USOM - BİLDİRİMLER - AYLIK



USOM - BİLDİRİMLER - YILLIK



<https://www.usom.gov.tr/tehdit.html>



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ

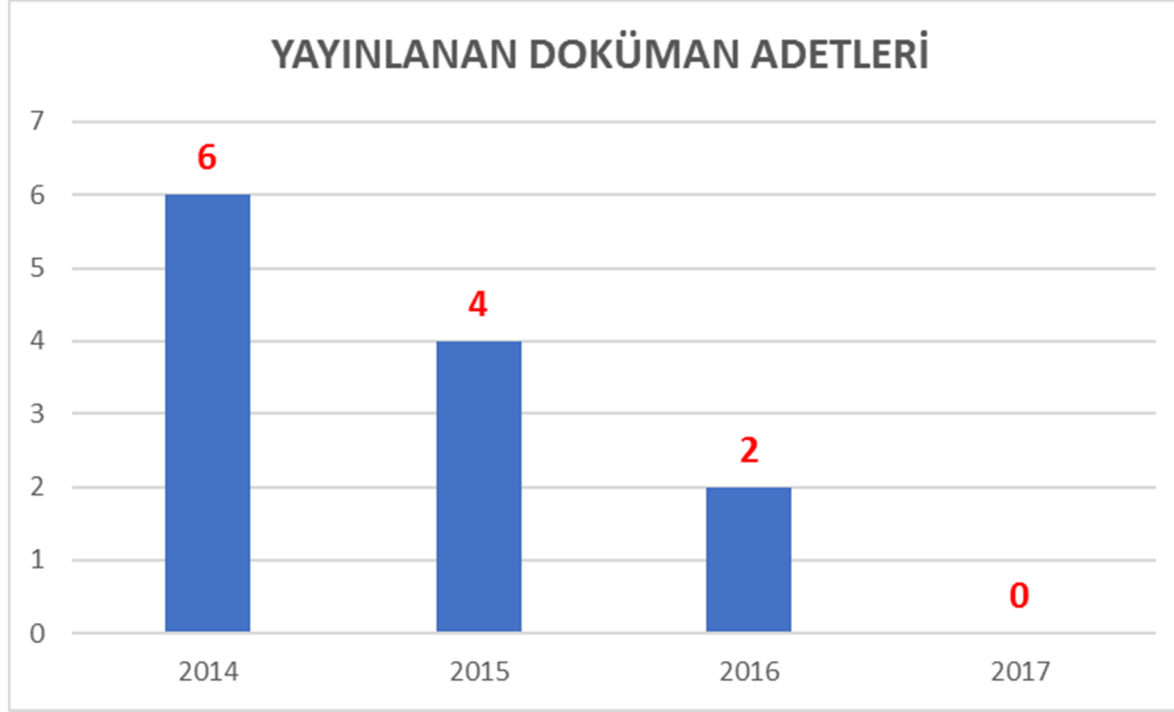


BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

SAYILARLA USOM



<https://www.usom.gov.tr/dokuman.html>



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

SAYILARLA USOM

+90 312 586 53 05 iletisim@usom.gov.tr



ANASAYFA | HAKKIMIZDA | GÜVENLİK BİLDİRİMLERİ | DUYURULAR | FAYDALI DÖKÜMANLAR | İLETİŞİM

IBM Güvenlik Güncellemeleri Yayınladı

Genel Bilgi

IBM; IBM Domino server IMAP EXAMINE türünde bulunan zafiyetleri gidermek için güvenlik güncellemeleri yayınladı.

Etki

Mevcut güvenlik açıklıkları nedeniyle siber saldırıların

Çözüm

Ulusal Siber Olaylara Müdahale Merkezi (USOM), kullanıcı ve sistem yöneticilerine IBM'in güvenlik bülteni ve CERT/CC VU#676632 kodlu zafiyet raporunu incelemelerini ve gerekli güncellemeleri yapmalarını tavsiye etmektedir.

İlgili Güncellemeler:

- Domino 9.0.1 Feature Pack 8 Interim Fix 2
- Domino 8.5.3 Fix Pack 6 Interim Fix 17

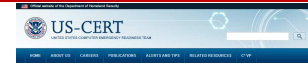
Kaynaklar

<https://www.us-cert.gov/ncas/current-activity/2017/04/25/IBM-Releases-Security-Update>

<https://www-01.ibm.com/support/docview.wss?uid=swg22002280>

<http://www.kb.cert.org/vuls/id/676632>

<https://www.usom.gov.tr/dokuman.html>



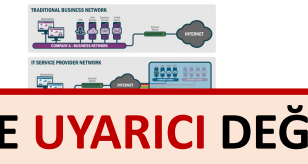
Alert (TAT-1714)

IBMdomino Affecting Multiple Victims Across Multiple Sectors

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

Systems Affected

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.



RESOLUTIONS

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

IBMdomino is a widely used email and messaging system. It is used by a wide range of organizations, including government agencies, financial institutions, and educational institutions. IBMdomino is a complex system with many components, and it is often used in conjunction with other IBM products. This complexity makes it a difficult system to secure, and it is often a target of cyber attacks. In recent months, there have been several reports of attacks on IBMdomino systems. These attacks have affected a wide range of organizations, including government agencies, financial institutions, and educational institutions. The attacks have caused significant disruption to the affected organizations, and they have also raised concerns about the security of IBMdomino. IBM has released a security advisory regarding these attacks, and it has provided information on how to protect your IBMdomino system. This advisory is available on the US-CERT website.

DAHA GENİŞ KAPSAMLI, SADECE UYARICI DEĞİL ÖĞRETİCİ

Ulusal Siber Olaylara Müdahale Merkezi

KAPASİTE GELİŞTİRME ÖNERİLERİ

- USOM, SOME'ler için daha güçlü ve **nitelikli bir bilgi kaynağı** haline gelmeli, ilgili kurumları bu amaç çerçevesinde koordine etmelidir.
- Daha çok **bilgilendirici rapor ve rehber** hazırlamalıdır:
İlgili **ENISA** Raporları, **NIST** dokümanları ve **CERT** Kılavuzları (*'First Responders Guide to Computer Forensics' gibi*) Türkçeleştirilebilir.
- **USOM ve üniversiteler** tarafından yapılan bu çalışmalar USOM sitesindeki **DOKÜMANLAR** kısmında kolay erişilebilir formatta yayınlanmalıdır.
- USOM sitesinde kamu, özel sektör, üniversiteler, STK, SOME ve USOM tarafından siber güvenlik alanında gerçekleştirilen/gerçekleştirilecek **etkinlikler** ve bunların sonucunda **elde edilen sonuç bildirimleri** yayınlanabilir.
- Webinar'lar sağlanmalı ve sitede **webinar kütüphanesi** oluşturulmalıdır. **Uzaktan ve 7/24 izlenebilen eğitim** yaklaşımı hedeflenmelidir.
- Üniversiteler ile işbirliği içerisinde **sistemik SOME eğitimleri** sağlanmalı, bu eğitimlerde mutlaka **pratik tecrübe oluşturacak lab'lar** yer almalıdır. «Olay Müdahalesinde Yapılan Yanlışlar ve Dikkat Edilmesi Gereken Noktalar», olay müdahalelerinde etkin görev alan kurum uzmanlarından benzer tecrübe aktarım eğitimleri verilmelidir.

«NASIL» ?

SİBER OLAYLARA MÜDAHALE EKİPLERİNİN KURULUŞ, GÖREV VE ÇALIŞMALARINA DAİR USUL VE ESASLAR HAKKINDA TEBLİĞ

11 KASIM 2013

Kurumsal SOME'lerin görev ve sorumlulukları

Madde 5: (2) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda **teknik ve idari tedbirler konusunda öneri sunarlar.**

(4) Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı **kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar.**

(8) [ve Made 7-(6)] Kurumsal (Sektörel) SOME'ler **7/24 erişilebilir olan iletişim bilgilerini** belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildirirler.



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

SOME'de NİTELİKLİ İNSAN KAYNAĞI

- **Siber Güvenlik, Veri Güvenliği, Kişisel Veri** Uzmanlıkları tanımlanmalı
- Üniversitelerdeki siber güvenlik alanındaki merkezler ve akredite edilmiş özel sektör eğitim merkezleri tarafından **uzmanlık sertifikaları** verilmeli
- Üniversitelerdeki siber güvenlik alanındaki merkezler, akreditasyon ile **uluslararası hedefler** belirlemeli: «**Küresel Kapasite Geliştirme Gücü**»
- Sertifika programları **pratik saha tecrübesi** de oluşturmalı
- Bazı **milli ürünlere özel uzmanlıklar**: "Pardus Göç ve Destek Uzmanı"
- USOM ve SOME'lerde **görev ön şartı** için **uzmanlık sertifikası + sahada pratik tecrübe** ön şart olmalı
- SOME Ekibi için **özel mali teşvik olmalı**: 7 x 24 Çalışma, Kritik Görev Alanı



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr

«TAM MİLLİ» SİBER GÜVENLİK

- Yazılımların **tam kaynak kodu** olmalı:
 - AKK şart değil (source-available / shared-source) ama kaynak koduna sahip olunmayan karakutu bileşen içermemeli : *Örnek - Milli Arama Motoru*
- **Milli özel sektör** tarafından hazırlanmalı:
 - Devlet sadece altyapı ve ARGE'yi hazırlamalı
 - Yazılım geliştirmede devlet özel sektörle haksız rekabet yapmamalı:
 - Devlet, yazılım geliştirme yerine bunlara altlık olacak **çerçeveler**, kütüphaneler ve ulusal **AR-GE** çalışmalarını gerçekleştirmeli, standartları belirlemeli
 - Milli özel sektör bunları kullanarak **sektörel** (sağlık, eğitim, ...) ve **yatay** (EBYS) yazılımlar geliştirmeli
 - 8227 sayılı Kamu İhale Kanunu **İstisnalar** - 3. maddesi, özel sektördeki **rekabeti** destekleyecek şekilde yeniden ele alınmalı
 - Sektör **seviyelendirilerek** kategorilere ayrılmalı
 - **Kamudaki pazar** bu kategorilerin gelişmesini sağlamalı
- **Sürdürülebilir** modeli olmalı:
 - Sadece AR-GE teşvikleri ile yalnız bırakılmamış, **ürün haline gelmiş çözümler**
- **Teknik, idari, mali ve hukuki** açıdan devlet tarafından desteklenmeli

STANDARTLAR - 27K AİLESİ

TSE Tarafından Türkiye'ye Kazandırılması Gereken Güvenlik Standartları

STANDART	AÇIKLAMASI	ÖNCELİK
ISO/IEC 27019	Enerji Endüstrisinde Süreç Kontrolü için Bilgi Güvenliği	★
ISO/IEC 27021	Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi güvenliği yönetim sistemi uzmanları için yeterlilik gereksinimleri	★
ISO/IEC 27032	Siber Güvenlik Rehberi	★
ISO/IEC 27034-1	Uygulama Güvenliği 1: Uygulama Güvenliği Rehberi	★
ISO/IEC 27010	Sektörler arası ve örgütler arası iletişim için Bilgi Güvenliği Yönetimi	★★
ISO/IEC 27033-6	Ağ Güvenliği 6: Kablosuz IP Ağ Erişim Güvenliğini Sağlama	★★
ISO/IEC 27035-1	Bilgi Güvenliği Olay Yönetimi 1: Olay Yönetim Prensipleri	★★★
ISO/IEC 27035-2	Bilgi Güvenliği Olay Yönetimi 2: Olay Tepkisi Planlama ve Hazırlama Rehberi	★★★
ISO/IEC 27036-4	Bilgi Güvenliği Olay Yönetimi 4: Bulut Servis Güvenliği Rehberleri	★★★

2017'de Siber Güvenlik, Milli Çözümler ve Türkiye «NE'LER, NASIL'LAR»

TEŞEKKÜR EDERİM

Mustafa AFYONLUOĞLU
Siber Güvenlik, e-Yönetişim ve e-Devlet Kıdemli Uzmanı
afyonluoglu[at]gmail.com
Linkedin: <http://linkedin.com/in/afyonluoglu>
Twitter: <http://twitter.com/#!/afyonluoglu>
Web: afyonluoglu.com



BOĞAZIÇI ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ



BThaber

TÜRKİYE'DE SOME'LER ve SİBER GÜVENLİKTE YERLİ MİLLİ ÇÖZÜMLER

8 Mayıs 2017 Boğaziçi Üniversitesi, İstanbul / siber.boun.edu.tr